Unclassified **NEA/CSNI/R(97)17**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 16-Feb-1998
Dist. : 06-Mar-1998

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Unclassified **NEA/CSNI/R(97)17**

Cancels & replaces the same document:
distributed 12-Feb-1998

Principal Working Group No. 5 - Risk Assessment

A COMPENDIUM OF PRACTICES ON SAFETY IMPROVEMENTS IN LOW-POWER AND SHUTDOWN OPERATING MODES

English text only

62013

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article I of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral. non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996) and the Republic of Korea (12th December 1996). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of all OECD Member countries except New Zealant and Poland. The Commission of the European Communities takes part in the work of the Agency.

The primary objective of the NEA is to promote co-operation among the governments of its participating countries in furthering the development of nuclear power as a safe, environmentally acceptable and economic energy source.

This is achieved by:

- *encouraging harmonization of national regulatory policies and practices, with particular reference to the safety of nuclear installations, protection of man against ionising radiation and preservation of the environment, radioactive waste management, and nuclear third party liability and insurance;*
- *assessing the contribution of nuclear power to the overall energy supply by keeping under review the technical and economic aspects of nuclear power growth and forecasting demand and supply for the different phases of the nuclear fuel cycle;*
- *developing exchanges of scientific and technical information particularly through participation in common services;*
- *setting up international research and development programmes and joint undertakings.*

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has concluded a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

* * * * * * * * * * * *

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France

ABSTRACT

Considering the extent of activity and number of safety improvements that have evolved over the past several years, CSNI Principal Working Group No. 5 - Risk Assessment initiated a task to update the 1993 State-of-the Art Report on Shutdown and Low Power PSA.

This new report provides a compendium of practices on safety improvements/enhancements in Shutdown and Low-Power operation modes in OECD Member Countries.

FOREWORD

Traditionally, the focus of safety assessment of Nuclear Power Plants has been on severe accidents during full power operation. It has been assumed that the risk originating from events during other modes of operation would be small in comparison with full power events. This perception has been based on the fact that the potential impact of an accident during low power and shutdown (LPS) conditions are lower due to decreased decay heat and that more time is available for recovering actions, should adverse situations occur.

During the last years low power and shutdown analysis has come into the focus of nuclear safety considerations. Operational experience and performance of Low-Power and Shutdown Probabilistic Safety Analysis (abbreviated LPS PSA or SPSA) have highlighted that the risk from those operational modes is significant and could contribute up to 50% to a total core damage frequency. Based on this considerations the OECD/NEA Principal Working Group 5 for Risk Assessment decided to form a Task Force (Task 13) to cope with this issue. It was decided that the Task Force should compile a report on plans, methods and experiences in the area from the different OECD countries.

The Task Force prepared and published its first report in 1993. That report was appreciated by many SPSA practitioners. As the activities in this area are developing rather fast, a review of appropriateness of the 1993 Task Force 13 report was undertaken. This review determined that many programs had advanced in the mean time and that an update of the 1993 report was needed.

The review of the 1993 document also pointed out that the advances had occurred in the area of implementation of findings of the SPSAs and other safety studies. An update of the 1993 Task Force 13 report focuses on both the techniques and in particular the measures taken to improve the safety in shutdown and low power operation.

This update of the 1993 Task Force 13 report was initiated in 1996, and was completed in 1997. As the update actually meant a complete rewrite of the report, the Task Force was renamed Task 97-1 “Risk Based Control of NPP systems during shutdown” Safety in shutdown operations-Compendium of practices on safety improvements”.

The Task Force leader of both the Task Force 13 and the new Task Force 97-1 was Mr. Bo Liwang, Head of Reactor Safety Analysis Division of SKI of Sweden. Other members of the Task Force included Dr. Lanore of IPSN, Mr. Versteeg of GNKK, Mr. Viroleinen of STUK, Mr. Szikszai of Paks NPP and Mr. Murphy of NRC. Additionally, the Task Group wishes to provide acknowledgement of the specific service of Dr. Bojan Tomic and the personnel at Enconet Consulting who provided much of the in-depth technical analyses as well as overall coordination in editing and compiling the report.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background to the Project

Operational experience and performance of Shutdown and Low-Power Probabilistic Safety Analysis (SLP PSA) have highlighted that the risk from those operational modes is significant. Based on this consideration the OECD-NEA Principal Working Group 5 for Risk Assessment decided to form a Task Force (Task 13) to address these issues. It was decided that the Task Force should compile a report on plans, methods and experience in the area from the different OECD countries.

As a result of this effort, the OECD-NEA issued a Report on "Shutdown and Low-Power Safety Assessment - a Status Report" in November 1993. This Report pioneered international work in this area. The Report was very successful in delineating topics highlighting the issues of concern and presenting the state of the art studies as available at the time. As such, it served an useful purpose to inform wider audience of SLP PSA practitioners, but also regulators and utilities on issues relevant for Shutdown and Low-Power Safety Analysis.

Considering the extent of activities on SLP PSA which have occurred since 1992/93, and from the today's perspective, the original Task Force 13 Report is outdated. In addition to specific SLP PSA studies, which are completed to-date, a number of studies have been initiated in several countries. Moreover, methodology has in the mean time matured.

The results of several SLP PSAs became available, and are being implemented at plants to improve the safety during Shutdown and Low-Power operating modes. In the 1993 Report, those issues were not discussed as the information was not available.

Considering the significance of the safety improvements in Shutdown and Low-Power operating modes, the extent of activity in the area over the last several years and the fact that methods are well profiled, the OECD-NEA Task Force 13 initiated an activity to develop an update of the 1993 report. The aim was to provide a compendium of practices on safety improvements/enhancements in Shutdown and Low-Power operation modes. In addition, this should be a continuation of efforts in compiling the plans, methods and experiences in the area from the different OECD countries.

1.2 Project Objective

The objective of this project is to identify the safety improvements related to shutdown and low power operating modes which were undertaken in different OECD countries. Special attention was paid both to different methods which are regularly applied to assess the safety in shutdown and to the results and findings which were used as a basis for identification and implementation of the safety

improvements/enhancements at different NPPs. The project also provided a listing of safety improvements/enhancements undertaken in 10 countries analysed.

1.3 Project Scope

The scope of this project is to generate a compendium of safety improvements/enhancements for Non-Full-Power operating modes which have been undertaken in selected OECD member countries. The compendium contains three broad categories of the safety improvements/enhancements:

A) ***Administrative actions*** (Administrative limitations and Technical Specifications, Configuration control),

B) ***Operational actions*** (Operating and Emergency Procedures, Work practices, training, etc.) and

C) ***Hardware improvements*** (Instrumentation and control. Alarms, other hardware).

Additionally, the scope of this project is to discuss in more detail the methods and approaches commonly used for assessment of safety in shutdown in OECD member states, and review the most recent status of the activities in the selected countries.

1.4 Structure of this report

The report focuses on an international outlook on the risk issues related to Shutdown and Low-Power conditions, including approaches used in the OECD countries to reduce the risk during Shutdown operating mode. Further, the application of those approaches to enhance the safety during shutdown and low power operation and specific measures undertaken at various plants are discussed:

This report encompass seven Chapters. Chapter 1 in Introduction.

Chapter 2 summarises the international experience on the use of different approaches to the assessment of risk during shutdown operating mode. It focuses on three main approaches: 1) “Full-Scope” SLP PSA models, 2) Barrier Analysis Approach and 3) Configuration control tools.

Chapter 3 focuses on specific modelling issues related with the SLP PSA. It provides an in-depth overview of international experience on modelling issues of interest, and experience in the use of a full-scope SLP PSA.

Chapter 4 summarises the NEA member countries activities in the area of shutdown and low power safety assessment, with focus on PSA.

Chapter 5 discusses the actual safety improvements related with the low power and shutdown operating mode. The discussion focuses on 3 major areas of improvements: Hardware, Administrative and Operational improvements.

Chapter 6 of this report provides the conclusions reached.

Chapter 7 lists References.

2. APPROACHES TO SLP PSA ANALYSIS

2.1 Background

During last few years, operational experience and performance of the Shutdown and Low-Power Probabilistic Safety Analysis (SLP PSA) highlighted the magnitude of the risk contribution from those, previously considered safe operating modes. This risk was found to be significant and, in some cases, contributes up to 50% to the CDF.

This risk is not related to the plant design. It is rather related to the unavailability of equipment due to maintenance activities undertaken during an outage, presence of additional (contractor) personnel who may not be fully aware of the safety issues, presence of additional heavy loads and flammable materials etc. All of these items increase the risk during plant outage.

Adequate planning and preparation of activities during outages can reduce both the probability and the consequences of possible events. In other words, there is a lot of possibilities for safety improvements in those operating modes. To decide what kind of improvements are the best on safety and cost beneficial grounds, a variety of analytical approaches could be used. One of these is administrative control based on the experience of individuals involved in the outage planning. While any careful analysis will find ways to improve safety during outages, it is felt that this approach would not be best suited to very well handle a more complex interface, since critical configurations may not always be recognised. Another approach is a PSA-type modelling, which considers a variety of interactions and dependencies of important systems.

PSA models are a highly useful tool for assessing the risk in the SLP operating modes. Many plants, especially in Europe, **use detailed Shutdown PSA models**, which address different operational states and initiators. Other approaches used include very simple (practically look-up tables) models called **Barrier Analysis**. Other, especially in the USA, use simplified train level models coupled with a presentation system called **ORAM** (Outage Risk Assessment and Management).

The selection of an approach and a model used for assessing the risk in the SLP operation involve addressing certain important issues related with the purpose and the scope of analysis.

Performance of any of the three types of approaches, and in particular PSA for Shutdown and Low Power Operating Mode, may support the enhancement of the safety during plant outage, and may contribute to reduction of the outage duration. Thus, a detailed analysis of shutdown operation may contribute to a more economical plant operation, improve plant safety and lower the consequences of incidents.

2.2 Full Scope SLP PSA Models

2.2.1 Background

The first full-scope Shutdown PSA studies performed were French studies for 900 MW and 1300 MW series NPPs. The results of those studies were widely published and have shown that actual risk during shutdown is in the same order of magnitude as the risk during the full-power operation. The results of French studies prompted a broad interest in application of shutdown PSAs, primarily in Europe.

The Full-Power PSA is no longer representative of the actual plant risk profile during the operational condition when the configuration of safety and support systems has changed extensively. This usually happens when the reactor power is below a certain level and automatic actuation of safety systems is being blocked (e.g. interlocks). Therefore, contribution of the risk during plant outage deserves a special attention and a "full-scope" SLP PSA appears to be an ideal tool to improve safety during plant outage.

Most of the studies completed to-date identified the areas of particular concerns like Mid-loop operation for PWRs or Cold Over-pressurisation for BWRs. Many of the SLP PSAs found that simple modifications like change in procedures or additional instrumentation could significantly reduce the risk during plant outage. Additionally, many studies highlighted the possibility for other cost effective solutions.

2.2.2 Objective of SLP PSA

The general objective of a SLP PSA is broadly similar to the power PSA. This includes a comprehensive overview of the plant risk (defined as a Core Damage Frequency if Level 1 is concerned). Additionally, the objective may include identification of design and operational weaknesses, propose modifications, evaluate Technical Specifications, etc.

Objectives unique to the SLP PSA are related to the analysis of specific activities which are taking place during an outage, or during low power operation. During an outage the plant configuration of both the Reactor Coolant System (RCS) and the safety and support systems are significantly different than those during power operation. The inventory in the RCS (coolant level) is changing, and some equipment is being taking out-of-service. The unavailability of different pieces of equipment often overlaps during the plant outage.

As the high risk situations are mostly due to simultaneous unavailability of systems, coupled with increased probability of disturbances, the main objective of the SLP PSA is to identify those high risk situations, and to provide feedback to outage management and/or to outage planning and control. Due to presence of a large number of additional temporary personnel on the plant site, who may not be enough aware of the safety related issues, another important objective of the SLP PSA is to define operating and emergency procedures to cope with sequences caused by human interactions.

A detailed discussion of the methods and approaches used in SLP PSA is presented in Chapter 3 of this document.

2.3 Barrier Analysis Approach

2.3.1 Background

The Barrier Analysis method aims at assessing the safety margin of the plant, given occurrences of a specific events. It is a systematic engineering approach designed to indicate the strengths of "barriers" which are available for a variety of events analysed. For the analysis of a shutdown operating mode, the Barrier Analysis was used by a utility in Sweden.

2.3.2 Objective of Barrier Analysis

The objective of the Barrier Analysis approach is to identify the most important active and passive safety barriers available to cope with initiators during an outage. Overall, the Barrier Analysis is used to assess the safety margin of a plant in presence of specific conditions or against undesirable events.

The information generated in Barrier Analysis is presented in a diagram illustrating the barriers available and their strength. The Barrier Analysis approach does not include quantification. The results are based on a **qualitative judgement** on the number of barriers and their strength, where strengths are assessed separately for specific barriers.

2.3.3 Barrier Analysis Method

The Barrier Analysis method can be characterised as an analysis of available barriers and their specific strength against a chosen number of undesired events. The concept of "undesirable events" also includes actions which may not lead to an accident, but reduce available Technical Specifications below adequate safety margins. As an example, the performance of a critical test with a safety system inoperable is an undesirable event.

Additional examples of undesirable events include:

- Primary system leakage,
- Criticality,
- Cold over-pressurisation of pressure vessel,
- Cold over-pressurisation of steam generator,
- Deviation from TS,
- Refuelling accidents, and
- Personnel injuries.

The Barrier Analysis is carried out in three phases and they are as follows:

- **Preparation,** selection of events and assessment of sequences,
- **Observation,** which includes plant information collection, and
- **Evaluation** of the results and preparation of the recommendations.

In the **preparation step** the most critical sequences during an outage are identified and selected for further analysis.

In the **observation step** selected critical evolution sequences are developed and the information collected in terms of systems and/or activities "preventing" the development of an accident sequence. In the final step, the evaluation, all information obtained is analysed and conclusions are drawn with respect to available barriers. The evaluation of results is based on identifying the number and the strength of barriers available, namely:

- Number of barriers available (technical, administrative, human action),
- Number of barriers with or without containment function,
- Sequence of administrative barriers, their strength,
- Analysis of barriers in terms of single failure criterion,
- Estimated potential consequences, and
- Time available for corrective actions.

2.3.4 Results of Barrier Analysis

For the final evaluation a **Barrier-Time (B/T) diagram** is used to show the barriers for each undesired event during different phases of an outage. A B/T diagram has a time on X-axis and a list of the different physical and administrative barriers against the identified undesired event on Y-axis. By comparing the B/T diagrams for the undesired events, the most critical sequences for every undesired event can be selected. The evaluation also has to consider the seriousness of the consequence of the event.

Recommendations for the improvements are given on the basis of assessment of the barriers available. Technical barriers are considered more reliable than administrative/human barriers. A consideration within the Barrier approach is that all suggestions for safety improvement should conceive the cost effectiveness of each improvement.

2.3.5 Conclusion

The Barrier Analysis approach aims at providing a fast alternative to determine safety related deficiencies of an outage in a systematic and transparent way. In addition to providing the results on its own, the Barrier approach could also be used for prioritisation of sequences to be evaluated within a full-scope SLP PSA. Due to its transparency, the Barrier analysis approach could also be useful for presentation of the SLP PSA results to plant personnel.

The Barrier Analysis is claimed to be successfully used in Sweden. It is now known if the application of the barrier analysis approach has been applied for the analysis of outage operations elsewhere.

2.4 ORAM (Streamlined Configuration Control type tool)

2.4.1 Background

Various operational applications of PSA related methods have been broadly accepted in commercial Nuclear Power Plants. One of the complex, but interesting and useful applications, from the utility perspective, is the use of PSA for configuration control. Such an application is typically called Risk Monitors.

The recent interest in Risk Monitoring for power operation has a different background in Europe and in the USA. In the USA the prime driving force behind Risk Monitoring appears to be both the financial interest (to reduce the cost of operation) and the safety interest. The most visible potential applications are: Configuration control, Maintenance-rule-related issues, and Technical Specifications. In Europe, as a centerpiece of discussion between utilities and regulators, the Risk Monitors are more safety-focused and attention is placed on risk follow-up.

Unlike power operation, one of the biggest issues in relation with the shutdown safety is configuration control. The Risk Monitor tools are well suited for such an application. The ORAM approach is the tool to help plant control and maintain their configurations. It was originally developed by EPRI in the early nineties as a response to concerns related to high risk evolution during outages caused by inadequate configuration control. As it proved to be instrumental in helping to reduce the duration of outages by 2-4 days without compromising safety, more than 40 USA utilities adopted it for outage monitoring. Its popularity in Europe is much lower.

2.4.2 Characteristics

The ORAM (Outage Risk Assessment and Management) grew from the Shutdown safety programs in the USA in the late eighties and early nineties. Unlike in Europe, where the assessment of risk in shutdown mode was, and still is, performed using traditional PSA tools, in the USA it was concluded that the configuration control (and related Technical Specifications) in shutdown are sufficient to control the risk. On the basis of the NUMARC guidelines, EPRI embarked on development of a tool to be used to identify high risk configurations in shutdown and provide the guidance on risk management.

EPRI sponsored development of ORAM software package which consists of Probabilistic Shutdown Safety Assessment (PSSA) and Risk Management Guidelines (RGM), both of which are used to identify and control safety in shutdown operating mode. The stated objectives of ORAM is to:

- Provide an easy-to-understand status of a **Safety Function,**
- Determine instantaneous risk at any time during an outage,
- Provide timely suggestions for preventing incidents, and
- Provide the mechanism to assess the effects of changes on the safety status and risk during an outage.

The ORAM software could be integrated with various outage scheduling software packages for automatic input of data to outage schedules.

The safety decisions in ORAM are based on a simplified plant status model which includes consideration of several safety systems/functions. Those are modelled using simple train level functional models. The evaluation of the risk during an outage is accomplished by dividing an outage in a series of discrete plant states defined by the Plant Operational Mode (POM), RCS inventory and RCS configurations. For each of those discrete states, the status of important safety functions is determined.

The safety functions monitored are as follows:

- Decay heat removal,
- Inventory control,
- Electric power,
- Reactivity control, and
- Containment.

The availability target required for each function and every plant state is determined by a decision logic contained in the Shutdown Safety Function Assessment Trees (SSFAT). The results are presented in a form of colour codes (red, orange, yellow and green), indicating the related degree to which the Safety Function is fulfilling a required target(s).

The colour determines the level of Defense-in-depth for every Safety Function (which in reality shows how many trains are available etc.). This, in fact provides an insight on how well the overall outage is managed. The software allows different queries and snapshots to enable the operator to investigate different proposed configurations.

The code also provides review of an outage once completed, as actual status of safety functions (unavailability) for every period in an outage could be stored.

For every state and function there is also a set of risk management guidelines. Those are the compendium of information on the risk significance for specific conditions. The risk management guidelines give instructions to the operators on possible responses to specific situations. Those are however, predetermined based on the pre-processed scenarios.

The PPSA is an integral part of ORAM. It is a grossly simplified set of Event Trees which links the frequency of initiators with the system/function status to determine the probability of a sequence. The end-states considered include core damage, core boiling, fuel pool boiling and possibly other states. The initiating events considered, are typically limited to:

- Decay heat removal failure,
- Loss of off-site power,
- Loss of AC bus,
- Reactor vessel isolation,
- LOCA, and

– Drain-down events.

The PPSA is used to identify the time dependent risk during an outage to support the risk management guidelines. The product of this part of ORAM is also a timeline graph, indicating the frequency for selected end-states at different time points during an outage.

2.4.3 Uses

ORAM was initially developed for two USA utilities (PGE and PECO) which also participated in the development. At present, ORAM is used or considered by more than 40 utilities in the USA and 2 in Europe. ORAM models are prepared during the outage planning phase, and modified as necessary during the outage. The outage schedule is accordingly reviewed and adjusted to achieve required safety level. ORAM is also used throughout the outage to control the safely level, especially for cases when some of the activities are delayed or similar.

A contributor to the popularity of ORAM in the USA is a need to reduce the outage duration. Any reduction of duration of an outage put more emphasis on prevention of critical configurations. Application of ORAM helped utilities to reduce the duration while assuring that the configurations are acceptable from the safety.

Active users of ORAM are attributing some of the reduction in outage duration directly to ORAM. Diablo Canyon and Limerick Nuclear Power Plants claim the reduction of at least 3 days in the last two outages. However, one European evaluation found out that, while reduction in duration of outages are likely in the USA where typical outage last for 6-7 weeks or even more, at European plants the typical outages are in the order of 4 weeks and similar effects may be less likely to occur.

2.4.4 Conclusion

ORAMs great advantage is in its simplicity and great presentability. Therefore, it is liked by the operators. Its simplified models and decision making logic is transparent to operating and maintenance personnel. Its results are presented in such a way to be easy understood to both plant staff and contractors. Those factors, coupled in real reduction in outage duration achieved at some plants (which is not to say that those could not be achieved by careful planning even without the ORAM-like tools), are contributing to the popularity of ORAM in the USA.

The drawbacks of ORAM may be primarily associated with its simplification. The models and as well as the quantification are simplified, and the treatment of dependencies and Human Errors (both of which are of the crucial importance in outages) may not necessarily be complete. When compared with full scope SPSAs, ORAM does not cover all the events which are typically addressed. The great advantage of ORAM is a very easy modification and maintenance of the models, and its on-line connection with outage scheduling tools. Unlike PSA which is usually prepared for an average outage, ORAM is developed for every specific outage, and moreover, is able to monitor every specific change during an outage.

ORAM is arguably a very useful tool for utilities to enhance the safety in shutdown mode, especially the aspects which are related with the configuration control. It contributes significantly to an understanding of the risk profiles during an outage, and thus has a positive effect on outage planning. The simplifications associated with ORAM are important, and needs to be properly understood.

3. MODELLING ISSUES RELATED TO SLP PSA

3.1 Introduction

This section discuses various modelling issues which are of relevance for a full scope shutdown and low power PSA models. The modelling issues discussed include the definition of plant operating states, initiating events, screening analyses, modelling of accident sequences, dependency analysis, quantification of sequences and applications of SLP PSA.

3.2 Plant Operating Modes and Plant Operational States

The definition of the "Plant Operating Mode" (POM) varies from country to country. Many countries have adopted the USA definitions, where Mode 1 is the power operation, and Modes 2 to 6 are various hot and cold stand-by or shutdown modes. Understanding of plant operating modes and its characteristics in terms of systems available and the general plant conditions is essential for the development of a SLP PSA. Operating modes are also highly important for defining the interface between power PSA and SLP PSA.

For an integral PSA model of a plant, it is significant to adequately define the interface between power PSA and SLP PSA. This interface does not necessarily coincide with the definition of the operating modes. Typically, the power PSA considers 100% nominal power. In terms of the thermal hydraulic response to an initiating event, there is not much difference between 100% power and lower power levels, except that at lower power levels the time available for selected corrective actions may be somewhat greater. The 100% power case is therefore conservatively a representative of the whole spectrum of power levels.

When the reactor power reaches a certain power level, the automatic actuation of the safety systems is disabled. Depending on the reactor design, and in some cases on operating practice, this could be between 2-10 % nominal power. This point is the natural interface between the power PSA and SLP PSA.

While the reactor is on low power, even without automatic actuation of safety systems, the power PSA models (with appropriate modifications) could be used to determine the risk level. This is generally true also for the hot stand-by mode.

Once the reactor is in the shutdown mode, and especially when the decay heat is removed via residual heat removal system (RHR), the state of the plant is such that most of the power PSA models are not applicable without major modifications.

The following table shows the Plant Operating Modes for a typical western design PWR.

Table 3.2-1. Plant Operating Modes for a Typical Western Design PWR

PLANT OPERATING MODES			RCS Pressure (bar)	RCS Temperature (C)	Duration (h)	Contribution (%)
A	AT POWER		154	304.6 Tm 286	7912	90.33
	START UP		154	286		
	HOT STAND BY	From nominal condition to P11/P12	154 138 P11	286 284 P12		
B B1	COLD SHUT DOWN (RCS press.)	Intermediate shut down RCS solid	30 23	120	123	1.41
		COLD SHUT DOWN	30 23	90 70		
B2	COLD SHUT DOWN (RC non press.)	DRAINED FOR MAINT. assimilated Mid-loop	P atm.	70 10	366	4.17
B3	REFUELLING	RCS open Pool filled	P atm.	60 10	301	3.44

Plant Operating Modes are important from the standpoint of the conduct of the plant operation. For a SLP PSA the plant operating modes do not mean much. Due to extensive changes in plant configuration during a shutdown period, it is necessary to define **"Plant Operational States"** (POS) which will properly reflect the plant configuration during an outage evolution. The POS is used to define "boundary" conditions within which there would be no changes in major characteristics which are important for PSA modelling.

Plant operational states are thus defined as a period during a plant operating mode when important characteristics are distinctively different from an another plant operating state. The important characteristics describing a plant operating state are:

- RCS temperature and pressure,
- RCS water level (inventory),
- Decay heat removal,
- Availability of safety and support systems,
- Containment integrity,
- System alignments, and
- Reactivity margins.

Some or all characteristics indicated above should be considered in defining the plant operational states. It is obvious that defining the POSs for every possible plant condition may result in a very large number of POSs. The attempt to define all the POSs which are relevant for SLP PSA could result in several hundreds POSs. One of the initial activities related to defining the POSs is their grouping to reduce the number of POSs to a manageable level. The grouping process shall consider issues like specific success criteria, typical IEs and system availability. The actual practice varies among PSA practitioners, but the general guidance is always to distinct POS in their main characteristic

A typical number of POSs considered in SLP PSA varies from a few to a few dozen with an average between 10 to 20. Today's state of the art indicates that a set of 15-25 POSs seems to be an appropriate number considering necessary level of details and a manageable size of the study. Newer studies tend to have more POSs than the early ones (e.g. Borssele SLP PSA has 28 POSs and Sizewell B SLP PSA has 30 POSs). It should be noted that the scope and objectives of a SLP PSA have a dominant effect on the selection of the POSs.

3.3 Initiating Events

Defining a list of initiating events is the major step, which influence the whole SLP PSA development process. While the main aim is similar to power PSA, actual initiators considered in a SLP PSA are different from those of the power PSA. The profile of initiators considered also highly depends on the actual outage considered (lengths and type; forced, refuelling, etc.).

Three broad categories of initiators (internal) are typically considered in a SLP PSA, and they are as follows:

- Loss of cooling,
- Loss of coolant (LOCAs), and
- Reactivity events.

To provide a comprehensive measure of the plant's risk, the SLP PSA should consider some additional initiators like: internal fire, flooding and drop of heavy loads.

Loss of cooling events represent a group of events which result in loss of heat removal from the core. When the core is cooled by the RHR System, it's failure is the main initiator in that group. Since loss of off-site power (LOOP) can also cause loss of RHR system, it is sometimes grouped within Loss of Cooling events.

Loss of coolant events are a challenge to the core integrity in the same way as during Full-Power operation. However, the profile and the causes of LOCAs are significantly different in the shutdown mode. In the shutdown mode breaks of pipes and reactor vessel rupture are still possible, but the dominant sources for LOCAs are the drain-down events, including inadvertent opening of valves, accidental pipe damages and similar. Both drain-downs to the plant rooms or to another system (intersystem LOCA) should be considered in a SLP PSA. Cold Over-pressurisation events which are challenging the integrity of primary circuit may be broadly grouped with this category.

Reactivity events are a specific category due to their specific issues and consequences. Reactivity accidents can lead to a local or a full core criticality. Examples like boron dilution, unintentional withdrawal of control rods or refuelling errors may be considered in the SLP PSA. International experience has shown that many such events occurred at NPPs, and their frequencies is high, though the consequences are low (recoveries are possible in many of those events). Some phenomena, like unborated slug of water entering the core and its consequences, are still being analysed.

Like in a Full-Power PSA, hazards can be divided into two groups, internal hazards and external hazards. Internal events include fire, floods and events like drop of heavy loads. These events in comparison to power state are differently treated in a SLP PSA due to their specific attributes.

Internal Fire have significantly higher frequencies in comparison to the power operation. The possible fire locations increases during an outage due to extensive maintenance activities. A fire during an outage is usually initiated by some repair work like cutting, welding or grinding, while fires during the power operation are usually initiated by electric circuits.

Flooding has increased frequency due to maintenance activities where floods would be caused by opening isolation valves and similar activities.

Drop of heavy load is an event which is seldom considered in the power PSA but it could have significant impact on the SLP PSA results. Numerous operations with overhead cranes has actually been analysed in several studies, although the results were not found to dominate the risk profile.

The basic principles for **determining the frequencies** of Initiating Events (IEs) are the same as for the Full-Power PSA. However, the determination of the IEs frequencies for Shutdown events is much more plant specific due to configuration, maintenance practices and other issues. In SPAS, sometimes the frequency of an IE would be dependent on POS, and would be determined for every (or a group) of POS individually. There are three basic approaches to determine frequency of an IE in a given POS. They are:

- Determination of frequency based on plant specific data,
- Determination of frequency by quantifying a logical model of an initiator, and
- Considering the Full-Power PSA IEs frequencies with additional analysis/justification.

Determination of the IEs frequencies based on **actual operating experience** (plant specific or type specific data) could be the most accurate approach but in the same time it is the most difficult one. A thorough evaluation of the records on various occurrences during outages is essential in determining the IEs frequencies. It is very important that the evaluation of experience is performed together with the plant outage personnel who could correctly interpret the information contained in the historical records. The outage schedule as well as POS defined in the previous step should be evaluated to identify the possibility of the occurrences on each specific initiator in every POS.

Most of the completed SLP PSAs found that human interactions are a high contributor to the frequencies of many IEs.

The frequencies of IEs considered in the Full-Power PSA may be only the starting point in defining the IEs frequencies for SLP PSA. Many of the Full-Power PSA IEs are not directly applicable and the frequencies may be significantly different during an outage.

In many SLP PSA studies the frequencies for LOCAs (LOCA caused by pipe rupture) are just adopted from the Full-Power PSA. Such approach causes some controversy as whether LOCAs frequencies should be modified to reflect that the systems are operating at much lower pressure (some analysts argue that non-pressurised primary piping will have the reduced pipe ruptures failure rate). In fact, the contribution to CDF from LOCAs caused by pipe rupture is found to be negligible in many SLP PSAs. LOCAs caused by human errors will be much more important.

In the SLP PSAs, the grouping is highly dependent on the POS and as a general rule the IEs are grouped within a POS. The overall intention of the grouping is to reduce necessary resources needed for analysis. Grouping which tends to produce over-conservatism would support the plant safety assessment and would be useful for regulators to determine the safety level during an outage, but it will make a SLP PSA less useful for outage management.

3.4 Screening Analyses

Compared to a power PSA, a full developed SLP PSA would have much larger number of different accident sequences. This is due to a large number of POS, each of which may have several IEs (even after their grouping). Such a large number of possible sequences would make a SLP PSA too difficult to manage, and in general not cost efficient. An important step in a SLP PSA project is screening analyses to identify important sequences and POSs which require more attention.

For a SLP PSA it is generally not advisable to embark on a complex modelling or specific Thermal-Hydraulic analysis before screening analyses. One may put too much effort into the sequences which are of limited interest.

Screening may be done in several different ways. The Full-Power PSA binning procedure may be used as a basis, or preliminary Event Trees or simplified approaches like Barrier Methods may be used.
An important issue relevant to screening analyses is the time available for recoveries. Long recovery times, which are associated with activities later in an outage (when decay heat is low) and with a high level of water inventory, are more appropriate to be screened-out. Generally, sequences with available recovery times longer than 24 hours could be screened out without much danger of leaving out important results. Sequences with very short recovery times, which are those earlier in an outage and which involve very specific system availability, shall not be screened-out because of their generally highly importance.

Screening process can be performed in two phases. After screening-out the clearly unimportant sequences, the draft event trees can be developed for remaining sequences. The remaining sequences then could be analysed qualitatively or/and quantitatively. The main idea of the whole process is to select sequences of higher safety significance and to reduce the level of details in modelling work for sequences with lower safety impact. At the end, similar event trees may be grouped together.

The final step in the screening process is re-grouping of POSs and initiators. The result of the whole process is a list of safety important POSs and IE groups. The SLP PSA requires iterative processing for re-defining and re-grouping POSs and IEs several times during the process.

Development of detailed accident sequences (including supporting TH analysis, HE and CCF analysis) is the most labour intensive part of the SLP PSA, and its aim is to focus on essential issues only. Establishment of a systematic screening procedure is the best way of removing unimportant sequences.

3.5 Modelling of Accident Sequences

The system fault trees models developed for the power PSA could, with appropriate changes (i.e. components and trains in maintenance), be used for SLP PSA. The logic of systems basically remains the same, but the conditional availability of components or systems may be significantly different.

The success criteria are less stringent, primarily due to lower decay heat levels. Thermal-Hydraulic analysis are recommended to determine the success criteria. Some of the success criteria may be adopted from previous deterministic analysis with some additional verification of the applicability of the assumptions.

Determination of the success criteria should take into account the following issues:

- Status of the primary circuit (water level, RCS open, etc.),
- Decay heat level,
- Containment isolation status, and
- Availability of protection systems and their mode of operation.

In a standard SLP PSA**, the event sequence modelling** is usually performed using event trees. In this case, the event trees developed for power PSA may be modified for use in SLP PSA. The modification will typically include removal of some headings (i.e. reactor trip) and relaxation of the others due to lower decay heat levels. Some new headings may be added to reflect operator actions which may not be possible during power operation.

Shutdown state also has some specific characteristics which are not modelled in the power PSA. Operation of the RHR system and related operator responses often requires the development of new sequence models. A longer time is available to operators to recover from initial failures. Possibilities to establish a non-conventional accident mitigation (as an example, supplying water into the open reactor vessel via fire water system) require from the PSA analysts to consider options which have not been addressed in the power PSA.

Development of accident sequence models for SLP PSA requires a close co-operation between plant personnel who are familiar with an outage and PSA analysts to assure that the all possible scenarios are appropriately modelled. Available accident mitigation measures may be much broader that for the power PSAs. The systems and the plant features which have been credited in power PSA may not be available for shutdown mode (as an example, heat removal using steam generators). The development of sequences should be an iterative process to adequately model sequences which represent actual plant configuration.

System modelling is usually performed by using Fault Trees. As in sequence modelling, the models developed for the power PSA could, with exceptions, may be used as a basis for SLP PSAs as well. Revision of the models is necessary due to the following:

- The system model for the power PSA describes a different system behaviour than that in the shutdown,
- System is operational in shutdown (it is in the standby mode on power),
- System actuation is manual (it is automatic on power),
- Mission time is different,
- System success criteria changes with POS,
- Redundancies are different in different POSs,
- Recovery possibilities are different, and
- System alignment is different for individual POSs (e.g. power supply buses, water supply, etc.)

In some cases it is more cost effective to develop a completely new system model than to modify an existing one.

Some systems may require specific modelling for a SLP PSA because they are not considered in the power PSA. An example is the Spent fuel pool cooling system. Some operating modes of the RHR system may be specific to a POS. System recoveries credited in power PSA may not be applicable due to on-going activities or due to limited accessibility, etc.

3.6 Human Interaction

Human Interaction analysis is the most important issue in a SLP PSA. Both the plant outage and the start-up activities involve a large number of operator actions, functional tests and maintenance activities. All of those have to be correctly introduced in a SLP PSA. In a SLP PSA 5 different types of Human Actions may be considered:

- Human actions before initiating event, affecting availability of equipment,
- Human actions as an initiators,
- Procedure based human interactions to terminate an event,
- Human actions in attempt to follow the procedure which failed to terminate an event, and
- Human actions to recover the failed equipment or to terminate an event.

Compared to the power PSA, human interaction analysis in a SLP PSA is much more complex since they require identification of actual ways the work is being done and consideration of interactions which are not obvious.

During the plant outage human actions can affect the safety in different ways, including:

- Human Action can initiate an accident; e.g. LOCA, power supply failure, and
- Human Action can worsen the situation during the course of an accident, e.g. failure to bring the mitigating system in operation.

In general the types of Human Actions during Shutdown operating mode or during plant outage are as follows:

- Pre-initiator Actions

  A) maintenance of various equipment

- functional tests and calibrations

  B) Post-accident Actions

  C) actuation of systems, the automatic actuation of which is inhibited

The following issues needed to be addressed when evaluating the Human Interactions during outage safety analysis:

- Lack of Technical Specification requirements and limits, and lack of Operating Procedures,
- Lack of supervision on maintenance activities,
- Lack of appreciation of risks during Shutdown, and

- Lack of comprehensive and appropriate training.

While performing SLP PSA the following steps are important for considering Human Interactions:

- Identify all possibly important Human Interactions during plant outage,
- Screen these Human Interactions and prioritise them from the risk perspective, and
- Collect Human Interactions information from plant experience during Shutdown operating mode, and establish Human Error data base.

3.7 Dependency Analysis

Dependency analysis for a SLP PSA follows the same basic principles as for the power PSA. During an outage, the dependencies tend to be much more complex than during power operation. Testing and maintenance activities during shutdown operation create new dependencies which need to be identified and documented by the SLP PSA analysts. Cross-connections and support system status may cause hidden dependencies which need to be taken into account.

The CCF analysis may also be more complex than for the Full-Power operation. The CCF mechanism and impact of maintenance has to be understood and appropriately modelled. An example is a four train system where two trains are in maintenance and two operational trains fail to start on demand due to a CCF. The concern is whether the maintenance activity has removed the CCF mechanism and could the trains in maintenance be recovered or not.

3.8 Plant Damage States

Classification and grouping of accident sequences into plant damage states follows the same basic principles as for the power PSA. The list of plant damage states is more extensive than for the power PSA.

Typically, the following plant damage states may be considered in SLP PSA:

- Fuel damage in reactor vessel/spent fuel pool,
- Boiling in reactor vessel/spent fuel pool,
- Extensive criticality,
- Local criticality,
- Cold over-pressurisation,
- Radiation over-exposure of workers, and
- Heavy loads collision.

The status of the containment may be of high importance in defining the plant damage states. For some plants the containment cannot be closed in a short time and any of fuel damages would directly result in an off-site release. Therefore, some SLP PSAs include containment consideration in the definition of the plant damage states.

3.9 Quantification of Accident Sequences

This task is similar to quantification in the power PSA. However, the sources of data as well as the procedure to develop a data base may be different.

Data for component unavailability for SLP PSA have significantly different emphases than that for the power PSA. While in the power PSA the unavailability of safety components are (often) dominated by the failures in stand-by, in SLP PSA they are clearly dominated by maintenance unavailability. Maintenance schedules and actual duration of various tests and maintenance actions need to be carefully evaluated to determine the actual equipment availability (of major systems specific POS depending on their status may be defined). For random failures, the failure rates used in the power PSA could be used (although some of the analysts argue that the random failure rates to be sued in SLP PSA shall be different that for power PSA, no conclusive evidence of such position has been demonstrated) .

Quantification of accident sequences, uncertainty and sensitivity analysis follow the same methodological approach as for the Full-Power PSA. Due to various influences, it was shown that the SLP PSA results typically have higher uncertainties.

3.10 Application of SLP PSA

The applications of SLP PSA are many, and some have been demonstrated. In addition to determination of the actual safety level during an “average” outage, SLP PSA is useful to provide various kinds of feedback. Some SLP PSA would be performed for two types of outages; a long outage with major maintenance and a short outage which basically focuses on refuelling and some minor maintenance.

Ideally a SLP PSA may used for the outage planning in an iterative way. The draft outage plan is assessed by a SLP PSA. Sensitivity studies are used to minimise the risk associated with certain tasks. The SLP PSA may be used to justify the moving of some tests and preventive maintenance from an outage to the full-power operation or to justify the selection of simultaneous or sequential testing practices

The following are considered as possible applications of SLP PSA results:

- Outage planning and scheduling,
- Operating and maintenance procedures,
- Technical Specifications,
- Accident procedures/emergency planning, and
- Decision on hardware modifications.

It has to be noted that a SLP PSA is not an ideal tool for day-to-day outage planning due its rather complex models. However, no other tool can mach the SLP PSA capabilities addressing dependencies, complex human interactions and similar phenomena.

During low-power operation and specially during an outage many activities are taking place with overlapping time intervals. A plant typically passes through a large number of different plant configurations. A SLP PSA is a highly useful tool to integrate this type of information and identify non-safe plant configurations. Unavailability of components, safety and support systems and containment isolation status can be effectively modelled by SLP PSA.

By identifying the risk significance of the unavailability of the safety and support systems, a SLP PSA may provide a feedback to the development of the additional Technical Specifications for outages.

During the performance of a SLP PSA, accident sequences which strongly depend on recoveries initiated by the operators may be identified. For those recoveries, emergency operating procedures may then be developed utilising SLP PSA generated insights.

Plant specific SLP PSAs were performed in many European countries (Sweden, UK, France, Spain, Switzerland, Finland, Belgium etc.) and in most cases were successfully used to avoid high risk configurations and to identify backfits for specific operating conditions. After implementing the backfits, the contribution of SLP PSA to the overall risk was often significantly reduced.

4. INTERNATIONAL EXPERIENCE WITH SLP PSA

4.1 Introduction

The following Chapter provides a summary of insights on the issues related to SLP PSA which were found to be of high importance. Using SLP PSA for decision making, assumptions and limitations must be properly understood. Insights may then be applied to the outage management and, in some cases, to hardware or procedural modifications.

The aim of this Section is to highlight the issues which were integral to bringing the plant to a high risk situation environment. Those issues are discussed from the point of view that their relevance is as a part of a SLP PSA study, to identify plant specific high risk configurations.

The following Chapter summarises some of the important points which were found critical high risk configurations internationally. Other Chapters of this section provide an overview of the activities related with the SLP PSA in selected OECD countries.

4.2 Findings

4.2.1 General findings

To date, dozens of safety studies for shutdown operating mode or outage conditions were performed world-wide. Those range from simple studies aimed at identifying causes (and frequencies) of losses of RHR function to full scope SLP PSA studies. Most of those studies were plant specific exercises. Many safety studies on outage conditions identified (and initiated the implementation) alternatives and procedures to deal with the high risk configurations.

During an outage, safety equipment may or may not be available, but almost certainly will depend on human interaction for its initiation. Administrative barriers like Technical Specification may be vague or non existent. The operating support from instrumentation to procedures and training may be inadequate. The disturbances to “normal operation” are typically more frequent than for the power operation; and caused by different initiators, mainly human interaction.

The technological processes and in general, development of accident sequences during shutdown is much slower that during power operation. Significantly longer time is available for recoveries and it is also possible to use non-standard systems and approaches to recoveries.

All those make the considerations of high risk configuration during shutdown operating mode significantly different than for the power operation. Moreover, the critical issues identified are highly plant specific and international experience could only be used as a reminder in this case.

With regard to **PWR type reactors**, the single risk-dominant configuration is the Mid-loop operation. The contribution of Mid-loop operation to overall risk, per unit time, is several orders of magnitude higher than the risk in the power operation. The main concern during the mid-loop is loss of heat removal (due to the coolant level reduced below the RHR Pump suctions) and rapid boiling in the core. Loss of RHR pumps due to vortex was identified as the most dominating single initiator in several studies. The remedial measures for this case range from installing new hardware to monitor the level in the reactor vessel, specific procedures and additional interlocks to forbidding (regulatory mandated) Mid-loop operation in periods when the decay heat level is high.

Loss of Power sequence, especially during maintenance of emergency diesel generators, is another important element. During outages, the full separation and drain supply is not always maintained. Studies found and operational experience confirmed that loss of a part of the power supply systems has caused complete loss of residual heat removal and similar. In this case, specific administrative limitation, like strict control of the power supply for the RHR pumps or the limitation of DGs maintenance depending on the availability of the second off-site power source were introduced.

Risk associated with reactivity incidents usually is not the most dominant one. However, its consequences and little possibility of recovery before some fuel damage occurs make reactivity incidents an important concern. The slow dilution incidents are well understood and often experienced phenomena. The administrative and hardware improvements were made at many plants to prevent slow dilution. Rapid dilution, like introduction of a slug of unborated water in the core is potentially critical incident. Some analysis performed in Germany found that such an accident could lead to a pressure peak in the reactor. Hardware interlocks and administrative limitations were introduced to reduce the probability of such an event. In France, the charging flow to RCP is terminated during loss of off-site power, to prevent the formation of the slug of unborated water which would be transported to the core when the pump is restarted.

The risk profile of a typical plant shows the peak at the moment of shutdown of the reactor and again at the start up. The peak at shutdown is related to switch over to the RHR System, and it is due to possible inoperability of the system which cannot be verified before the system's operation is required. This phenomena is well understood and the measures to reduce the risk are mainly related to assuring the diversity in heat removal (like steam generators full with water, etc.). The risk peak at the start-up is often related with the cold over-pressurisation event which is especially dangerous during the water solid conditions, when inadvertent safety injection or malfunction of charging systems can cause major rupture of RCS. Interlocks and procedures were developed and employed to cope with this phenomena.

With regard to **BWR type reactors**, the single risk-dominant initiator is the cold over-pressurisation. There is potential for cold over-pressurisation during filling the reactor at the end of a Shutdown sequence. The status and proper actuation of safety and relief valves were found very important for BWR type reactors during shutdown state.

Pool cooling system, fire water system and make-up water system are usually available and can be used to mitigate accident sequences. However, in some cases these systems have no safety related requirements, and consequently, the pool chemistry and cooling systems are not safety classified.

4.2.2 Internal Fire

The operation experience of nuclear power plants internationally shows that more than 90 % of all fires on NPPs occur during plant outage.

There is a lot of difference in fire events for power operating mode and for shutdown .A fire during the plant outage is usually initiated by some repair work; for example, by some cutting or welding. At that time most of the safety systems, possibly also including the fire protection system, may be fully or partially out-of-service. Fires during power operating mode are typically initiated by electric current (failure in electric systems) and most or all of the safety systems are available to minimise the consequences.

Fire analysis can be performed to a different level of details. The approaches on this vary from study to study. In many fire analysis conservative assumptions are made, e.g. when fire occurs in a certain room all components in the room are lost. These assumptions may not necessarily be applicable for shutdown operating mode. During plant outage there are a lot more people in the plant that could either detect or extinguish the fire, though the automatic fire detection system may be out-of-service at that time. The fire analysis for plant outage should also considered that the fire zones during power operation could be different than in shutdown.

Additional specifics to be considered when performing the fire analysis during an outage include:

- There might be additional fire loads due to maintenance work presence at the plant site,
- Fire barriers may not be available; fire doors may be open due to maintenance work, and
- Success criteria are unique to outage conditions.

4.2.3 Risk Related to the Spent Fuel Pool

The major source of radioactivity in a plant is the reactor core. Thus, safety analysis typically focuses on the reactor core. During refuelling operations, part or whole of the core is unloaded in the spent fuel pool. The decay heat contained in fuel elements shortly after the shutdown is such that without adequate cooling, the spent fuel in the spent fuel pool could overheated and ultimately melt. Many of the safety studies for shutdown included the analysis of the spent fuel pool. In fact, some of the studies found that the fuel damage in the spent fuel pool dominate the overall risk profile.
Generally, there are three different locations of spent fuel pool in NPPs:

- Separate fuel pool storage Building,
- Inside reactor building but outside containment, and
- Inside containment.

Consequently, the safety analysis of the spent fuel pool is different for each of those because of different IEs and different systems which are necessary to prevent or to mitigate the fuel damage.

The spent fuel pool model may also have some other peculiarities associated with it. As an initiating event the fuel handling failures may be taken into account. One of the specifics of the risk related to the Spent Fuel Pool is that the typical time interval until fuel damage occurs is relatively long (this depends on the water inventory and on the amount of fuel stored inside the pool), so that various recoveries can possibly be made.

While performing SLP PSA the following issues should be considered:

- Use of the RHR System for cooling the pool; reduction of available trains during maintenance activities,
- Spent fuel pool drain-down via cavity and/or RCS and interfacing systems,
- Transport of heavy loads across the fuel pool during shutdown, and
- Unloading patterns related to different outage categories.

4.2.4 Loss of RCS Inventory

The RCS inventory is essential to maintaining the overall decay heat removal function. During reduced RCS inventory operations, boiling and potential core uncovery may occur in a relatively short time period. The RCS boundary expands during plant outage, which usually includes decay heat removal piping, spent fuel pool, refuelling channel and other connected support systems.

There are a number of event sequences including the leaks or sudden opening of the valves, catastrophic failure of seals (cavity) and similar, which should be considered in SLP PSA that involve loss of coolant inventory due to a variety of causes, because of their importance, because those often lead to high risk configuration situations.

Safety studies performed to-date on NPPs internationally clearly indicate that the reduced inventory situations are the most critical periods. Special attention should be paid to loss of RCS inventory events, especially during mid-loop operation for PWR type reactors**.** The mid-loop operation represents a higher risk condition due to reduced RCS inventory. Any additional impact on RCS inventory may have crucial consequences. A loss of coolant during low RCS inventory is an event where the recovery times are minimal, and an event could develop to an accident within minutes.

The frequencies of IEs related to loss of inventory are important input to SLP PSA. Care must be exercised when adopting the data from the power PSAs. In such cases, the different operating conditions must be observed.

4.2.5 Loss of Residual Heat Removal

Most of the time during shutdown operation the safety function depends on RHR system. During shutdown operations and due to various maintenance configurations the RHR System has many “single” failure potentials. The importance of the RHR System is especially evident during the mid-loop operation (for PWR type reactors) due to reduced RCS inventory when a variety type phenomena could easily occur.

The operational experience has shown that the Loss of RHR Function could be caused by a variety of events, from losses of power and other support systems to failures within the I&C System and similar. Furthermore, the loss of RHR function could (and in many cases was) be caused by human interaction issues, like closing isolation valves, erroneous train/flow path manipulations, transfer, etc. All such possible causes are extremely plant specific, so a careful assessment needs to be performed to identify all such issues which lead to high risk configurations.

4.2.6 Other

Besides the issues discussed in previous Chapters there are other configurations and/or potential contributors which were found of importance at selected plants, and this may require appropriate attention in analysis. They are as follows:

- Sequences resulting in cold over-pressure affect the reactor vessel integrity,
- Heavy load drops affect the integrity of barriers (RCS, containment),
- External events during shutdown may turn to a high risk contribution, since the containment barrier does not exist, and
- The boron dilution events may lead to prompt criticality resulting in fast pressure increase, jeopardising the RCS integrity.

4.3 Summary of Countries Activities

The summary of activities related to safety analysis of shutdown and low power operating mode for selected OECD countries is presented in following chapters. The discussion focuses on highlighting specific activities (methods and approaches) in SLP PSA or other studies which may have been undertaken.

4.3.1 Country's Activities - Finland

Major SLP PSA study for Olkiluoto NPP (SEPRA) was completed in December 1992. Since that time, improvements have been done to SEPRA, including fuel ex-core analysis. Use of the specific analytical techniques "Analysis of Test Influence" (ATI) and "Human Action Deviation Analysis" (HADA) appears an important issues towards completeness of SLP PSA. A Level 2 study was initiated in 1994 and a more comprehensive Fire Analysis and Loss of Off-site Power during Shutdown in 1995/6.

In addition to determining the Core Damage Frequency (CDF), SEPRA study determined the probabilities for 8 other hazards during refuelling from criticality to mechanical damage of fuel. These issues are often seen as not important from the safety perspective, but are very important from utility's point of view, since it can cause significant financial losses. The SEPRA study is pioneering example in this area.

The results of SEPRA study have been used for implementation of several improvements and for initiation of few actions. Restricted personnel access to the lower equipment hatch during the main circulation pump overhaul was established and preparedness was increased by two special trained guards. In addition, procedures and Technical Specifications have been modified. Altogether, various modifications caused a decrease in CDF by a factor of 10.

Another Finnish NPP, Loviisa 1-2 (2 Units WWER 440), is developing its regulatory-mandated SLP PSA project. The project is initiated in 1994.

Some enhancements of safety in shutdown have been initiated, but those were not based on results of SPSA, than rather on the basis of operational experience. During the course of the identification of hazards, several items were noticed, where immediate changes of the operating procedures were possible (primary loop level control procedures, several test procedures, etc.). The preliminary findings of Loviisa SLP PSA have resulted in improvements of Operational and Test Procedures, and/or in some improvements of Technical Specifications.

4.3.2 Country's Activities - Sweden

Original Swedish "Barrier Analysis" approach was used on two NPPs, Ringhals 4 and Forsmark 2. These were limited scope studies evaluated selected predefined events such as main circulation pump overhaul, cold over-pressurisation, refuelling, control rod drive overhaul, testing and inspections.

A standard SLP PSA study was developed for Ringhals 2 NPP by Framatome. The original results of the study determined a very high CDF with the dominant sequence being loss of RHR during mid-loop operation and failure of operators to recover. Detailed sequence analysis found that alternative heat removal paths could be used. The model was re-quantified and CDF reduced for about an order of magnitude. Specific procedures, instructions and control were introduced with regard to mid-loop operation and some specific operating modes.

Several measures to further reduce the CDF in shutdown were proposed, including the monitoring of RHR pumps vortex phenomena, water level monitoring, etc.

Barseback NPP completed its shutdown study, which was reviewed by the Swedish regulatory body SKI, and found to be of a good quality. Even before the shutdown analysis, Barseback initiated various activities aiming at enhancement of safety during outages. Interesting ones are the definition of every outage as a project (which require specific safety analysis) and definition of "umbrella" schedules, where a series of interconnected systems or trains are maintained at the same time. A shutdown study is also underway for Ringhals 2 NPP.

4.3.3 Country's Activities - Germany

In Germany, the Regulatory Authority does not require performance of a plant specific SLP PSAs. The effort concentrated on limited Shutdown analysis on typical PWR and BWR reactors. For a typical BWR reactor, a coarse study was completed in 1992. The detailed study is still on-going and rather limited information on it are available.

In 1992 Siemens KWU developed a specific analysis of operational events during shutdown for typical German PWR reactors. The study was limited to the analysis of a refuelling (unplanned outages as well as outages for major modifications were not considered). The emphasis of the analysis was LOCA events inside and outside containment. A total of 6 POS have been analysed. The conclusion of the analysis was that the risk during outages does not much contribute to the overall risk of operation of NPP. It is believed that due to a higher level of automation, German typical PWR NPPs would generally show a lower CDF.

A specific aspect of shutdown safety which attracted more interest in Germany than elsewhere is related to a reactivity incidents. More specifically, a fast deboration sequence (a slug of unborated water, which

accumulates due to primary coolant pump seal injection with unborated water, is suddenly transported to the core). After several years of analysis using sophisticated thermal hydraulic codes, it was concluded that even in the worst case, the event would most probably not result in a large scale damage of the RCS nor the core damage. Some operators in Germany, introduced specific procedures to deal with this issue. One of proposed solutions is an administrative requirement to terminate the seal injection flow if a loss of off-site power occurs.

Specific studies were undertaken on the applicability of operational events analysed with SLP PSA on German reactors.

4.3.4 Country's Activities - The Netherlands

The SLP PSA study for Borselle NPP was completed in 1994. It turned out to be one of the major studies as far as the applications of innovative methods and approaches. The study considered both internal and external initiators and Level 2 Analysis. Limited Level 3 Analysis was partially performed.

The study considered two types of outages considered: long cycle type and short cycle type. It was found that the differences are small and mostly depend on the duration of the cycle. As in other SLP PSAs, mid-loop operation is a high contributor. Fire is the dominant initiator in terms of contribution to total CDF for non-power state.

The results of SLP PSA were used for establishing the safety improvements which were mostly related to procedures and Technical Specifications. An outcome of SLP PSA is that the maintenance on Borssele "bunker system" (additional safety systems located in an external events-proof bunker) is rescheduled to be undertaken during non-critical phases of outages. The availability of "bunker system" during critical phases of an outage greatly contribute to the reduction of overall risk. The original design of the "Bunker System" did not envisage use of it during outages

Another Dutch plant, Dodewaard, also has a comprehensive SLP PSA analysis. The results of this analysis (completed in 1994), were not available. It is known that the study was a major international activity, with specific methodological development and innovative approaches. Dodewaard plant is being closed down for decommissioning, so no measures focused at improvement of safety in shutdown were implemented.

All Dutch PSAs were reviewed by the IAEA IPERS team.

4.3.5 Country's Activities - Belgium

The SLP PSA analysis for two Belgium NPPs, Tihange 2 and Doel 3, have been completed in early 1993. The scope of SLP PSAs included full Level 1 internal initiators and limited Level 2 analysis. No external events were analysed.

Studies considered a total of 8 initiators, where 5 were adopted from the power PSA and 3 were specific to shutdown state. The results obtained are in line with results of other studies for similar plants, with contributions of 24% and 35% to the overall CDF for Doel 3 and Tihange 2 respectively. Mid-loop operation was found the most significant contributor for both plants.

The results of these studies initiated safety enhancement which resulted in reduction of risk for shutdown and low power operation. The improvements concentrated on enhancement of emergency operating procedures, Technical Specifications and test procedures. The shutdown EOPs, were improved for Doel NPP and a totally new set was developed for Tihange NPP. The modification of Technical Specifications

was related to the availability of ECCS which is now required to be available and aligned for hot leg injection when entering the mid-loop operation.

The test procedure for certain check valves, which were not regularly tested and therefore appeared to be critical contributors to CDF for LOCAs, was implemented/developed. The decision was made to install the test lines and establish a test procedure to mandate testing of check valves at least once per year.

PSA projects for other Belgian plants are completed and undergoing reviews. All PSA in Belgium include the SLP PSA models.

4.3.6 Country's Activities - France

Both French studies on SLP PSA (900 EPS and 1300 EPS) have been completed in 1990 and widely published. The results of those studies were presented and discussed at various forums world-wide. The results of the French studies initiated some immediate safety improvement measures for shutdown operation. Initially, temporary fixes were introduced, and which were later replaced with permanent installations.

The backfitting measures implemented include hardware modifications (e.g. automatic water makeup in case of loss of RHRS water level measurement in the RCS, etc.), administrative requirements establishing strict limits on specific actions in relation to specific time after shutdown and installation of additional automatic controls during shutdown. In France, significant attention has also been put to the analysis of criticality accident by an unborated slug of water.

Another interesting activity of relevance to outage safety (although not related to SLP PSA) is the use of operational experience as a basis for decision making on specific limits during shutdown. As a result of several repetitive incidents, strict limits on the time after shutdown when the entry into the mid-loop operations is allowed were imposed. This highlights the issue of use of operating experience as a basis (or as a background) for assessment and improvement of outage safety.

A complete reassessment of SLP PSAs has been carried out by EDF and is under review by IPSN - This review includes independent evaluations. The new results of SLP PSAs will be discussed and if necessary complimentary modifications should be performed.

4.3.7 Country's Activities - Switzerland

The Swiss Regulatory Body (HSK) requires that for every operating NPP, the plant specific PSA should be extended to include the probabilistic modelling of shutdown and low-power operations. As of December 1996, SLP PSAs have been completed for Goesgen, Muehleberg and Beznau plants. Leibstadt study is expected to start soon. The Swiss Regulatory Body HSK is performing full scope review of these studies.

Goesgen SLP PSA study considered three different outage types, 14 POS and more than 100 initiators. Additional thermal hydraulic analysis were performed to support the modelling of shutdown operations. Plant operation history as well as Siemens/KWU data for PWR were reviewed and used in the study. The most important initiators, in terms of contribution to CDF, is a loss of operating RHR (RHR cools the reactor and the spent fuel pool) pump, while redundant pumps are in maintenance, followed by internal fires. The operational practice at Goesgen NPP is to unload the core to the spent fuel pool during an outage. The results highlighted relatively high probability of damaging the core while in the spent fuel pool. This probability was in fact much higher that the probability of core damage during power operation.

However, the risk profile indicated a possibility of simple fixes to enhance safety and significantly reduce the probability of core damage (i.e. rescheduling of maintenance activities), which were immediately introduced.

Muehleberg study considered a selection of internal initiators and screened external initiators. The process of development of SLP PSA for Beznau was initiated through a preliminary (or screening) study. Interesting characteristics of Beznau SLP PSA is that the large volume of plant specific data is being collected in the framework of the study. Both studies were completed and submitted to the regulatory body for review.

4.3.8 Country's Activities - United Kingdom

The PSA project performed for Sizewell B NPP is one of the most comprehensive PSA projects undertaken. The whole PSA study encompass Level 1, 2 & 3 analysis, internal and external initiators, and all power states. The results and findings from this study served as a basis for the development of Technical Specifications for shutdown state as well as some more specific operating and emergency procedures. Some hardware improvements, including alternate relief paths, and instrumentation were also introduced as a result of the PSA model for shutdown and low power.

Another activity related to Sizewell NPPs is development of ORAM model which is to be used for outage planning for all outages at Sizewell site. ORAM was used at the first outage at Sizewell in 1996, and found to be very useful in both the planning process and the monitoring of configurations during the outage (including the changes to original configurations). Sizewell is one of only two European NPPs which use such a model in outage planning (other one is Krsko NPP).

At the present there is no plans to develop a Shutdown study for other reactors in UK. These reactors are refuelled on-line. For gas cooled plants Shutdown state is believed to be less important than for water reactors. At the present the UK Regulatory Body does not require any specific SLP PSA studies for those reactors.

4.3.9 Country's Activities - Spain

The Spain Regulatory Body (CSN) requires that all NPPs in Spain append their PSA projects with plant specific SLP PSA. The first plant which completed the SLP PSA (1995) is Vandellos 2, where the analysis of operating modes other that power were already within the scope of the comprehensive PSA project. The on-going PSA project for Trillo also has SLP PSA as an integral part. This study is expected to be completed in 1997. Two other Spanish NPPs are completing their plant specific SLP PSA; Asco and Jose Cabrera. All those plants PSA project is undertaken by a plant/utility analysis team with some support form external consultants.

The CSN requested from all other plants to bring their PSA projects to the same level as Trillo (which also includes all external events and Level 2) in the future.

4.3.10 Country's Activities - United States of America

The major US-NRC sponsored studies for Grand Gulf NPP and Surry NPP have been completed and their results published in NUREG 6143. Those studies were a multi--million dollars R&D efforts aimed at developing the state of the art methods and approaches which could eventually be applied for other NPPs in the USA.

The interest is shutdown safety in the USA started in mid eighties and was triggered by operational events during shutdown operation, mainly losses of functions like RHR or power supply. One of the first comprehensive analysis was a RHR reliability study for Zion NPP in mid eighties. The study concluded that the risk during shutdown operation exist but it is significantly lower that for the power operation. Another study with even broader scope was performed for Seabrook NPP. Those studies are not comparable in their scope with current modern SLP PSAs. However, the results clearly indicated that the mid loop operation is the most critical configuration, and that there is a need for maintaining redundancies even during the shutdown. The Seabrook plant was backfitted (mostly improvements of procedures and administrative regulations, but also some hardware improvements/enhancements) even before its commercial operation and the risk during shutdown mode (which was even higher that for the power operation) was reduced to an acceptable level.

The US-NRC does not require utilities to perform their plant specific SLP PSA studies, but in the light of operational events which occurred during shutdown state, the USNRC Rule on "Shutdown and Low-Power Operation" was proposed aiming at strengthening configuration control during outages. The USNRC felt that increased administrative and other control by the licensees would assure that the redundancies needed to cope with operational events during outages are sufficient for maintaining acceptable safety level during outages. The Rule was originally proposed in 1994, and its second , modified version was open for public comments in 1996. The discussion between the USNRC and the industry are still on-going and the Rule is not yet adopted.

The requirements for stricter control of configuration in outages helped the development and utilisation of configuration control tools like ORAM, which is now used by majority of the USA plants. Although the USNRC does not license the use of ORAM, it generally looks favourably to utilities using this (as well as other) configuration control tools. ORAM is discussed in details in Section #2 of this report.

4.3.11 Country's Activities - Canada

With significantly different design and operational practices, Canadian reactors (CANDU) with their on-line refuelling and separated coolant and moderator circuits do not appear to have safety problems of shutdown operating modes. The Canadian Regulatory Body (AECB) is not requiring SLP PSA type studies. In the future, there might be some more comprehensive evaluation of outages activities, including a possible application of SLP PSA type approaches.

A RHR operability study was developed for Darlington NPP in late eighties. This limited scope study concluded that there is no immediate safety concern related with the design or operation of that system, but indicated some weaker points which could be enhanced.

4.3.12 Country's Activities - Japan

Two activities related to Japanese SLP PSAs have been reported to-date. One is a MITI-sponsored "Level 1 PSA for Typical Japanese 1.100 Class PWR and BWR Plants During Low-Power and Shutdown Operation", and another is the activities related to assessment of the decay heat removal system at LMFBR plant.

The MITI-sponsored used the standard PSA approach (small event trees/large fault trees), THERP for human reliability calculation and the US generic data base except for Japanese-specific data for DGs. The final results were not available. The interim results for PWR and BWR plants are as follows:

For the PWR type reactor, a total of 17 POS were defined and 5 groups of initiators considered for their applicability in each POS. The results for PWR showed that mid-loop operation contributes about 80% to the CDF, and mid-loop operation with nozzle dams installed is the largest single contributor. The total contribution of the loss of RHR to the CDF is about 90%.

For the BWR type reactor, 3 groups of initiators were considered; loss of RHR, LOSP and LOCA. The LOSP group of initiators contributes to about 60% of the total CDF, mainly due to LOSP when one of the two redundant emergency power train is on maintenance.

The LMFBR study is not the SLP PSA in the real sense. The purpose of the project was to analyse the condition changes on the plant state in relation to failures or unavailability of RHR System. Instead of fault trees, the Monte Carlo simulation was used to model the transition. It is claimed that “Use of Monte Carlo simulation and transition time sampling method resulted in development of improved Shutdown PSA methodology, which is able to deal with condition changes of unplanned plant configurations”. Such a claim is made in a conference proceeding and for the purpose of this study it could not be confirmed.

5. SAFETY ENHANCEMENT IN SHUTDOWN AND LOW POWER OPERATION

5.1 Background

Safety of low power and shutdown operation received high visibility internationally after the results of early SPSA studies were published. Some of the safety issues related with outage operations and specific safety issues during shutdown were recognised earlier, both on the basis of specific studies (like RHR operability studies in the USA in mid eighties) and operating experience (operational events during shutdown). Some regulators and reactor owners groups initiated their own investigation and analysis of shutdown operations aimed at enhancing safety.

Considering the results of both operability studies and SLP PSA studies and international operating experience for low power and shutdown, many plants world-wide embarked on a variety of activities aimed at enhancement of safety in those operating modes. While the actual background ("source") of an improvement is not always easy to determine (if an improvement was decided upon the finding of a SPSA study or operational experience or vendor's advice) it is obvious that most of the improvements were implemented or proposed after the high risk contribution from shutdown operation was revealed by SPSA studies.

The improvements/enhancements during shutdown and low power operation may be divided into three broad categories:

- Administrative,
- Operational, and
- Hardware.

Administrative and *Operational* improvements/enhancements are sometimes overlapping and it is difficult to strictly define boundary between them. In many cases *Operational practice* depends on or/and is related to *Administrative restrictions*.

Many similarities in identification of problems and issues were observed internationally. However, it is obvious that the solutions are highly dependent upon the reactor type and general operating practices in specific countries or even specific plant. An illustrative example is the typical German practice with PWR reactors, where the whole core is unloaded at the beginning of an outage, with which, the mid loop operation risk becomes irrelevant. Most of the other PWR reactors find mid loop operation the risk dominant issue.

The following sections discusses some of the commonly identified problems and their solutions. While this review is not attempting to be an all-inclusive overview of all issues relevant for shutdown, it is believed that it provides a quite representative sample of major issues which are considered internationally.

To structure the presentation on different solutions accepted or considered at various plants, the discussion of specific improvements in all three areas of interest (*Administrative, Hardware, Operational*) is divided in four categories which may be considered the key for safety during outages at NPPs. Those are:

- minimising the probability of a disturbance (an initiating event),
- increasing the availability of systems to cope with IEs (including both the dedicated and the alternative systems),
- enhanced recovery capabilities (either increasing the available timing for recoveries, recognition or actuation capabilities), and
- enhancement of the containment function.

Each of those four major categories is further divided to allow for grouping of available information. The specific improvements undertaken in each of three major areas (Administrative, Hardware and Operational) are discussed for each of those 4 categories. The review indicates how similar problems may be addressed in different manner. A more detailed comparative listing of improvements is provided in the Appendix A.

Appendix B provide a detailed discussion on specific improvements undertaken by specific plants in all of 10 countries evaluated.

The following sections discus common issues which are relevant for improvements in three major areas. The discussion of relevance for every individual safety area is presented.

5.2 Administrative Improvements

Both the safety studies for shutdown and low power operation and the operational experience of plants world-wide have confirmed that the human interactions of various kinds are significant contributors to the overall risk level. This is naturally the consequence of more human interactions during shutdown (both maintenance and operations, as most of the automatic signals are blocked or disconnected) but also the fact that most of the plants internationally have relatively few administrative limitations and requirements as compared to the power operations.

The shutdown state was traditionally considered the safe state of the reactors so the technical specification requirements were seen as not necessary. That lead to the fact that very little administrative control was in place to assure the availability of systems and equipment. Moreover, the outage scheduling was in most of the cases centered on maintenance activities with less regard to available redundancies etc.

Newer plants, in general, tend to have more developed technical specifications for shutdown operations. Some plants have modified their technical specifications to address the shutdown operations. Those technical specifications would then tend to follow the same format as for the power operation.

The technical specification is a preferred way of dealing with the shutdown safety issues in the USA. The USA regulators determined that the technical specification requirements would be appropriate for assuring the safety in shutdown. Most of the European countries required utilities to perform a PSA study and identify possible improvements for shutdown operations.

Increasing popularity of Technical specifications for shutdown clearly indicate that the shutdown safety is to a large extent the configuration control issue. Technical specifications in most cases introduce somewhat rigid requirements, which is somewhat detrimental for shutdown operations, where the necessary availability of equipment and allowed configurations depends highly on the decay heat level etc.

An approach to configuration control in shutdown is use of risk monitoring tools like ORAM. Such a tool (which, because it was developed by EPRI, attracted much higher popularity in the USA than elsewhere, see section #2) allows a utility to optimise an outage (and reduce its duration) by maintaining a configuration which would guarantee low risk. Moreover such tools allow for modelling of changes in outage schedule and adjustment in configuration to maintain required safety barriers.

Another form of administrative control of safety in outages is the preparation of a Shutdown safety plan or operational plan for an outage. Such plans are prepared specifically for every outage. An outage operation plan would contains list of systems and timing when specific systems shall be in operation or an active standby conditions. Even before performing their shutdown safety studies, many utilities would prepare such plans for an outage. After risks related with shutdown operations were recognised, such plans may get more detailed, and in particular may address additional redundancies or diversities.

Shutdown safety plan is an extension of an outage operational plan to contain the risk management consideration. This would primarily list possible recovery actions considering systems and equipment which is or may be available at different periods during an outage.

Among the countries and plants analysed, there are different approaches to administrative limitations during shutdown. Those depends both on the reactor type and on the overall regulatory approach in a country. Most of the plants introduced some shutdown-operation relevant additions to their technical specification. However the extent of those appears to vary significantly. Administrative barriers are sometimes considered significantly “weaker” that the hardware barriers, so for the critical areas, the hardware improvements would be introduced. The administrative limitations, however, would be focused on assuring the availability of additional redundancies, or limitation of duration of specific operating modes (e.g. mid loop operation).

Specific administrative improvements dealing with each of the areas of safety interest are presented next.

1. Minimising the probability of an IE

The administrative barriers are useful in reducing the probability of occurrence of an IE during shutdown. Many plants internationally reviewed their technical specifications to asses the applicability for shutdown operation, especially considering the results of SPSAs. However, the administrative barriers are not considered the most effective improvement for this particular issue. Some more details on how the administrative barrier is used in certain situations is provided below.

A) LOCA

During shutdown, the most probable cause of a LOCA event is an inadvertent draining of the reactor by creating an opening below the core. The contribution to the frequency of LOCA from pipe breaks is considered to be very small. Administrative controls are primarily used to assure that the order of the primary circuit openings is maintained. By doing so, specific phenomena (like siphon effect) which would lead to the LOCA could be prevented.

The Administrative barriers are important but not the dominant means of reducing LOCA events during shutdown.

B) Loss of RHR

Loss of cooling events are the initiators with the highest frequency in shutdown. Administrative limitations relevant for loss of cooling are primarily focused to assuring the full availability of RHR system when entering the RHR cooling mode.

The Administrative barriers are important but not the dominant means of minimising the frequency of losses of cooling.

C) Loss of power

The focus of the reduction of the probability of a loss of power event to assuring that more (additional) power sources are available. The administrative barriers as technical specifications are very effective in that respect. Typically, the technical specifications would require the availability of the specific off site power sources or availability of certain number of emergency diesel generators.

After some incidents involving losses of power during shutdown, many plants did extend their technical specification to cover for availability of power sources. Typically, redundant off site power will be required in relation with the maintenance of an on-site power sources, and increased availability of power sources would be required when the plant is in a critical configuration, like mid-loop operation.

D) Reactivity incidents

The reactivity incidents of concern in shutdown operation are mostly the fast dilution incidents, which result in a rapid reactivity increase in the core. These are usually related with the transport of the slug of unborated water in the core after starting up a RCP. The prevention against such an event could be made by administrative barriers but also by hardware changes or an operational procedures. An example of an administrative barrier is the requirement for the isolation of a CVCS injection flow in a case of the loss of power event. Similar requirement is covered at other plants by a procedure (an “operational improvement”)

Administrative barriers are typically used for a prevention of (slow) boron dilution. Most of the plants would have a Technical Specification requirement on the boron concentration and its verification during the shutdown operation. In addition, there is an example of administrative requirement on the minimum permissible redundancy of neutron flux monitoring system detectors.

E) Over pressurisation

The over-pressurisation events may cause a serious problem at both PWR and BWR reactors. Those events could be dealt with by administrative, hardware and procedural improvements.

The plant technical specifications are typically defining the pressure/temperature limitation which are applicable during shutdown operation. In addition, some plants have backfitted their technical specifications to prohibit the use of specific pumps (i.e. those with high head delivery) to fill the reactor, or require the operability of adequate relief capacity during periods when the increased risk of over-pressurisation exists.

2. Increased availability of systems

The administrative requirements related with the prescribed availability of the systems are arguably the most effective way of assuring that the plant protection is available to cope with the operational events. Technical specifications extended to shutdown often define the minimum required operability of specific safety and support systems. This operability is usually lower than required for the full power operation, and depend upon the specific time in an outage. The main use of the configuration control tools, like ORAM is exactly in this area. The ORAM-tool will help assure the minimum needed availability of systems depending on the specific decay heat level and other conditions.

A) Heat removal

The typical administrative requirement focused at the enhancement of the availability of the residual heat removal function is the requirement to maintain the availability of the steam generators and then in the reflux cooling mode. The availability is to be maintained until the RCS is open. Some SPSAs found that the availability of SG before major opening of RCS significantly reduce the overall risk.

Other alternative cooling methods which are being required to be available include spend fuel pit cooling systems and bunker systems. SFP cooling is of importance for plants where the SFP is within the containment, and the SPF cooling could be lined up to cool the core. Some plants have constructed bunkered systems to cope with external events. Those bunkers would typically be unavailable for the whole of the outage. SPSA studies have shown that availability of bunker systems would greatly reduce the portability of accidents in certain plant operating states. Therefore, administrative requirements to have bunkered systems available was introduced.

B) Inventory control

Equally important are the administrative requirements for the inventory control. Those include a requirement for the availability of the safety injection (usually low pressure) and accumulators or the core spray systems for BWRs. Many plants have found that the maintenance on those systems could be successfully implemented during the period of low risk (i.e. core unloaded). Administrative requirements would be imposed for selected systems to be available when the risk is higher.

Another interesting requirement is related to the availability of water sources in case of LOCA. In some cases during an outage, the source of water for the core cooling would be limited (due to maintenance activities), and possibly not sufficient in the case of a LOCA. Administrative requirements may significantly reduce the probability of unsuccessful response to an IE.

C) Others

Administrative improvements related to the mitigation systems include mainly a more systematic approach to outage planning where "umbrella" schedules are being developed covering a series of systems, to prevent opposing unavailability of trains of front line systems and support systems.

Many plants performed systematic reviews of their Technical Specification for outages and brought those in a format compatible with TS for power operation, and included the specific requirements relevant only for outages.

3. Enhanced recovery capabilities

The administrative requirements related with the enhancement of the capability of recovery are primarily meant to ensure that the configuration when the personnel has a short time to mitigate an event are rare. Administrative requirements are well placed for improvement of time available for recoveries, as due to lowering the decay heat level, later entry in critical configurations like mid loop operation would visibly reduce the probability of non-recovery.

A) Increased time available for recoveries and early warning

Administrative requirements are imposed to prohibit entry into specific configuration before the decay heat is below a certain level. Typically, the decay heat would be related to the coolant inventory in a way to require a minimum time before the core uncovery (or boiling etc.) following the loss of RHR. Administrative requirements would assure a longer availability (and thus higher probability of a successful recovery). By limiting the duration of the reduced inventory configurations the risk of core damage is reduced.

B) enhanced status control

In selected cases, administrative requirements would be imposed to enhance the status control. This would typically require continuous display and monitoring of selected parameters of interest in control room. In some cases, the technical specification will impose the surveillance requirements on parameters of interest.

4. Improved confinement function

The administrative requirements are the only requirements designed to cope with the containment function in outages. This is obvious considering that the request for the containment function would be of interest only after an accident has already progressed beyond certain level. Typically, the administrative requirements would include the demand for a containment function to be available during critical configurations (like mid-loop operations).

At least one plant requires the containment to be closed during the mid loop operation. However, the requirement that the containment is re-closeable in a short period of time is more usual. Such a requirement is aimed at assuring that the containment equipment hatch, if removed, would be stored on a location which would allow for its closure within one or so hour.

5.3 Hardware Improvements

Similarly to administrative barriers, the hardware barriers for shutdown are less stringent than that for power operation. First, most of the systems are not designed for outages (and are required to be maintained typically during the outage), and secondly, the instrumentation and controls are focused on power operation and not on outages.

Even before SPSA and other safety studies were performed, the issues related to lack of appropriate hardware became obvious. Some of the incidents and accidents during shutdown clearly pointed out to the inaccurate level measurement in reactors (which could lead to a vortex and loss of cooling) and to the temperature monitoring in the core (where, in one event, the water in the core heated up almost to the boiling point, which was not recognised in the control room, because the instrumentation was outside the core).

The hardware improvement for shutdown operation is mostly related with the instrumentation and controls. Those include also the installation of various interlocks and similar, aimed at preventing events like draining of the reactor. Some isolated hardware improvements are related to specific line-ups or additional equipment needed to connect systems which could be used in emergencies (like connection for the well water to be used for the ultimate heat sink).

Another area of hardware improvements is actually related with maintenance tools and equipment. In some cases the way the maintenance is done on major equipment could jeopardise the safety of an installation. To cope with this issue, the maintenance equipment is being redesigned to reduce the probability of specific occurrences (like cotter pin to prevent lifting of a recirculation pump).

Hardware improvements are an important contributor to safety in low power and shutdown. While hardware improvements and additional equipment is clearly the best way to avoid some of the main problems related to shutdown operation (like water level measurement for mid loop operation) hardware improvement to be effective has to be combined with both administrative and procedural improvements.

The discussion below focus on the specific hardware solutions which are implemented at selected plants to enhance the safety in shutdown.

1. Minimising the probability of an IE

The hardware improvements are highly important to minimise the probability of IEs. In particular, hardware in form of additional instrumentation and interlocks is the best solution related with monitoring the water level in reactor or preventing the overpressure events.

A) LOCA

Hardware improvements to reduce the probability of LOCA appear to be mainly related with BWRs and focused on improving specific maintenance related tools and equipment to prevent LOCA caused by displacement of the recirculation pump or its seal. Other recorded

hardware improvements are hard wired interlocks designed to prevent opening of specific isolation valves on the piping connected with RCS.

B) Loss of RHR

Losses of RHR are the most frequent IE in outages. Within this IE group, the losses of RHR due to loss of suction of RHR pumps is the most frequent category. Loss of suction is directly related with the low level in the RCS, and most of the hardware improvements are focused to the control and monitoring of the water level.

Considering the probability of losses of RHR, the most critical period is the mid loop operation where even a small deviation in the water level could cause a loss of suction. Many plants (regardless of their SPSA or other safety studies) decided to install water level monitoring systems. A typical choice is the ultrasonic level measurement system. Some of the systems are the mobile ones (installed only during the outages) and another are fixed subsystems, permanently installed.

The actual operational events with the loss of RHR suction is in the most cases due to the inadvertent draining, i.e. draining of the RCS below the minimum level. The hardware improvement to reduce the probability so such events are focused on providing the interlocks to automatically terminate the draining upon a low level signal. Some plants increased the minimum permissible level in the RCS, and other reduced the setpoints for the RHR pumps trip on vortex.

C) Loss of power

No specific hardware improvement was identified to be implemented focusing on reducing the likelihood of losses of power.

D) Reactivity incident

Some hardware improvements were implemented to reduce the likelihood of boron dilution events. Similarly to the RHR related issues, the hardware improvements here are mostly focused on the instrumentation and interlocks. The instrumentation for the surveillance of boron concentration with alarms in the control room and modification of the charging flow intakes are examples of possible solutions.

E) Over pressurisation

Typically, the RCS has enough capacity to relieve the over-pressure, but the setpoints or the availability of relief valves (those may be blocked during an outage) is the issues. Hardware solutions are rare, though at least one plant engineered a diverse pressure relief path.

2. Increased availability of systems

Hardware improvements are to a lesser extent used to improve the availability of systems in shutdown. Most of the hardware improvement are related to additional instrumentation or automatic actuation capabilities.

A) heat removal

Loss of ultimate heat sink is a potentially critical event for plants which relay on water which is supplied through a long channel. One such plant (which already experienced a loss of cooling water) implemented the hardware modification which would allow for a well water (the well is located at the site) to be used as the ultimate heat sink. At another plant several hardware improvements were implemented to enhance the reliability of the RHR system.

B) Inventory control

The inventory control during shutdown typically relies on the operator to diagnose the problem and then to initiate an appropriate action to replenish the water lost. Both of those activities are subject to an operator error, and in a case of short time available for recovery could be a dominant contributor. A hardware modification to automatically initiate the RCS waster supply after a loss of RHR (upon the low water level signal) was installed at one plant.

C) Others

Plants equipped with bunkered systems often choose to maintain those systems during outages. Administrative limitations are sometimes introduced to assure that the bunker is maintained operable during the outages, or at least during the critical configurations of an outage. In addition to providing redundant (and sometimes diverse) water supply and cooling capabilities during outages, the real advantage of bunkered systems is their usability in relation to the internal or external hazards. Internal hazards like fire and flood are more frequent during outages than during power operation. Use of bunkered systems may be the only available safety function in the case of a major fire or flood during an outrage. One plant introduced a hardware modification to assure automatic initiation of bunkered systems for external events in shutdown.

Another plant increased the availability of ECCS system by installing the test lines for the check valves. Another plant embarked on the use of condition monitoring system to determine a real need for maintenance activities, thus reducing the maintenance related unavailability.

3. Enhanced recovery capabilities

Hardware improvements aimed at enhanced recovery or diagnostic capabilities are mostly related with the instrumentation, alarms and similar.

A) Increased time available for recoveries and early warning

Cavitation of a RHR pump may lead to pump damage and a loss of the RHR. One plant installed an alarm to warn the operators on the cavitation on running RHR pump allowing them, to initiate the appropriate action before the damage is to occur.

B) enhanced status control

Enhancing the operator information system may be the key to recovery of any potentially dangerous situations. At one plant, specific instrumentation and alarm was installed in the control room for the permanent monitoring of the waste level in cavity and RCS. Other plants performed a systematic review of alarms and signals in the CR during the outage and improved signals and alarms related with the water level in the RCS to assure longer available response time for operators in case of loss of RHR system during mid loop operation.

4. Improved confinement function

No specific hardware modifications were identified related with the improvement of the containment function. This is understandable, as the containment function as such exist (but is open during the outage as the equipment or the personnel hatch may be opened), and its use during outage could be fully covered by the administrative requirements, as it was actually done at several plants.

5.4 Operational Improvements

Operational improvements for shutdown operating state discussed here are primarily the operation and emergency procedures and the training of operators and other personnel. Enhanced procedure and improved understanding of the shutdown risks are key elements in enhancing the outage safety at many plants.

Similarly to administrative barriers, operational guidance for shutdown was generally lacking at many plants. Safety studies and actual operational events in shutdown triggered the development of outage safety plans and training of personnel to understand the shutdown risks. Many utilities introduced a systematic evaluation of outage plans to identify any safety detrimental activities and correct those.

Operating and emergency procedures for outage operations are targeting both the reduction of a potential for incident and the mitigation measures. Many plants performed reviews of all of their operating procedures to identify if any of those would lead to an unduly increase of a probability of occurrence of a potentially high risk situation. Those procedures would then be modified or specific backstop ruled developed. Some plants developed and implemented specific emergency operating procedures for mitigation of accidental situations.

Training of NPP staff and contractors to understand the outage risks is seen as an important contributor to shutdown safety. Many plants introduced the shutdown safety as a topic for the pre-outage training of staff. Some plants introduced the training on specific topics, aimed at both recognising the risk significant situations and mitigating eventual disturbances or events. Another aspect of training is the preparation for the mitigation of specific events, for example closure of the containment or specific manipulations.

The operational improvements are of particular importance in prevention of occurrence of events or in mitigation of events where enough time for recovery exist. The operational improvements are best used in parallel with the specific hardware improvements, where procedures would be developed to initiate specific actions following the alarms. Training activities are important to increase the understanding of the plant personnel and contractors of the safety issues related to conduct of outages.

1. Minimising the probability of an IE

A) LOCA

LOCAs caused by inadvertent draining are the most probable LOCA events during an outage. Introducing procedures which would focus on the draining process as well as the manipulation of systems connected to the RCS is one of the ways to reduce the probability of a LOCA. At one plant, the test procedure for the isolation valves was reviewed and modified to assure that a LOCA would not be caused by a test on isolation valves. Another plant modified the inspection practice of control rods to reduce the probability of draining the reactor.

B) Loss of RHR

Operational improvements focused on prevention of losses of RHR were mostly related with the changes of the water level in the reactor which could cause a vortex on the RHR pumps. Some plants introduced the procedures focusing on the verification of the water level, other enhanced the procedures governing the drainage operations.

Another way of reducing the probability of losses of RHR is to establish a requirement for a clearance from the control room for the specific activities. At one plant, a clearance from the CR was required for any manipulations with the SG nozzle dams.

To reduce the probability of loss of RHR caused by a failure of the RHR system itself, one plant introduced the limitation in manipulation of systems and equipment which are supporting the operation of RHR.

C) Reactivity incident

The operational improvements focused on the reduction of the probability of reactivity incident are related to better control of boron concentration. The highest concern is the injection of deborated water through the RCP seal injection. One plant implemented a procedure to isolate the injection flow after trip of a RCP. Another plant introduced a procedure which require additional verification of the boron concentration before the start-up of a RCP.

It is interesting to recognise that for the same goal (in this case reduction of a probability of a reactivity incident) some plants have selected to introduce procedures while other selected to implement an administrative limitation.

D) Over pressurisation

Reduction of the probability of over-pressurisation incident is one of the areas where operational improvements are the dominant choice. Specific procedures which were implemented by selected plants covers the equipment to be used for filling the rector (for example limiting the use of high pressure pumps) as well as define the specific sequence of activities to be followed.

E) Others

Other areas related with the reduction of probability of occurrence of events during shutdown operations are mostly related with the training of personnel to understand the risk related with the outage operation, and modification of specific procedures. One plant reviewed and modified all the procedures related with conduct of tests during shutdown, and another modified the practices related with the lifting of heavy loads. Some plants are defining every outage as a "project", which means that the safety aspects of activities undertaken during an outage are individually evaluated.

2. Increased availability of systems

A) heat removal

Use of procedures is a highly important aspect for increasing the mitigation capabilities (this actually covers both the system availability and recovery capabilities). Many plants introduced specific emergency operating procedures to cope with specific losses of function (like loss of coolant, Loss of RHR). Those procedures would address both the recovery of normal systems and use of alternate systems and cooling modes. One plant have a procedure for flooding the reactor after the loss of the RHR. Another has a specific procedure which allows for use of all three redundancies when the core is in the vessel.

B) Inventory control

Operational improvement for inventory control are mostly focused to alternative ways of mitigation of a LOCA event. One plant developed a specific procedure for using gravity feed from RWST in case of a low inventory in the RCS.

LOCAs (and other events) during low power, hot standby or hot shutdown modes are usually not well covered by procedures which are focused on power operation, mainly due to the fact that many automatic actions are disabled because of a low reactor power. At least one plant performed a systematic review of the operational procedures for LOCA in modes 3 and 4, and adjusted those to specific low power conditions. Other plant developed a specific EOP for small LOCA in shutdown. Another plant developed specific operating instructions focused on mitigating a small LOCA before the RCS level drops below the mid-loop level.

C) Others

Other interesting operational improvements for shutdown operation include a general review of applicability of procedures, development of an "umbrella" system of activities and development of specific post maintenance testing schemes. Development of an operating plan for shutdown which would indicate the required operability of systems and equipment could also be considered among operational improvements (some plants may call this an administrative improvement).

3. Enhanced recovery capabilities

A) Increased time available for recoveries and early warning

Time available for recoveries is of key importance for a successful recovery. For shutdown operations, most plants are introducing the administrative requirements for entry into specific sensitive operating modes (like mid loop operation). In some cases, operational improvements like specific procedures may also have an effect in increasing available time for recoveries or early warning. One plant developed a specific set of instructions for operators to mitigate the boron dilution events before those lead to criticality. Another plant (a BWR) posted specially trained guards to perform an immediate recovery action (closing the access door) in a case of large LOCA below the core. This would provide an immediate warning of the LOCA and an immediate mitigation action (in fact that was the only mitigation action which could be fulfilled in a short time).

B) Other

Operational improvements in this area include the "Operational commitments" data base, purpose of which is to highlight the safety relevant aspects of the outage activities. This data base would collect all the safety requirements which need to be observed during an outage and thus enhance the recovery from any incident during an outage.

Another plant introduced specific procedures focused on mid-loop operation which would enhance the recovery capabilities.

4. Improved confinement function

No specific operational improvements were identified for containment function. This is expected, as the procedures for closing the containment openings exist, so the administrative requirements for the application of existing procedures was enough to solve the containment issue for outages operations.

6. CONCLUSIONS

Increased interest in safety during shutdown operation of NPPs was triggered by both the publication of pioneering SLP PSA (French studies in this case) which showed that the risk contribution from those operating modes is far from negligible, and by several operating events which, in some cases in the USA, caused declaration of even site emergencies. The safety during shutdown operation was identified as being due to specific operating practices and less to the design of plants. The safety concept of all western plants which are in operation at present relies on a series or redundant and diversified safety systems to cope with initiating events. In addition to significant automatic actuation, operators have available extensive instrumentation systems to provide accurate information on the status of process and equipment.

These concepts are not maintained in shutdown. Automatic actuation is blocked. Systems are out of service because of maintenance. Operators have less instrumentation operable, and some of the key variables are even not monitored. Safety studies and engineering analysis of operational events clearly confirmed those insights.

Because of all that the safety enhancement for shutdown operation are (relatively) easy. Operation of systems which exists, but were in extended maintenance, could be assured by administrative requirements like technical specifications. Operators have generally enough time to perform the recovery actions in case of an event, though their extended training and specifically designed operational procedures would greatly enhance their capabilities and significantly decrease the probability of their failure. For critical parameters, additional instrumentation and monitoring systems (like water level in RCS or core temperature) were added, with mobile or fixed instrumentation in the control room. All those measures individually and collectively resulted in significant reduction of the shutdown and low power contribution to overall risk.

The review of actual safety enhancement focused on shutdown and low power operations presented in this report clearly indicate that there are different possible solutions for similar safety concerns. The improvements selected by specific countries and plants point out to different preferences or conveniences. While some countries concentrate on administrative improvements, other appear to favour interlocks and information systems. Some prefer training and operator information tools, other develop and put in practice the emergency operating procedures.

This report provides a compendium of information on both the studies and analysis undertaken and specific improvement practices. While specific practices may not be easy to adopt at other plants, it is believed that this report will foster an exchange of ideas and considerations for selection of adequate safety improvements at NPPs in OECD counties and beyond.

7. REFERENCES AND OTHER SOURCES

7.1 References

1. "Practices Implemented on the Tihange's Site for the Mid-loop State"; Internal Note, Tihange NPP, November 1996.

2. "Summary of (?)"; Internal Document, KGB Gundremmingen NPP, January 1995.

3. "Low-Power Level Safety Management of Finnish BWR"; Antii Piirto, Pekka Pyy, Leena Norros and Lasse Reiman; ANP 1992 Conference, Tokyo, October 1992.

4. "Shutdown Risk Analysis - Lessons and Views"; P. Pyy and R. Himanen, SRA Europe, Fourth Conference, Rome, October 1993.

5. "Experience from Shutdown Event PRA (SEPRA) for TVO I/II"; Risto Himanen, Jari Pesonen and Heikki Sjovall; IAEA TCM, Stockholm, November - December 1992.

6. "Applications of Low-Power and Shutdown PSA in France to Reduce Loss of RHRS Risk at Mid-loop Operation"; B. Tarride, IPSN/DES.

7. "Seabrook Station Probabilistic Safety Study Shutdown Modes 4, 5 and 6"; James H. Moody Jr., Thomas J. Casey and Kenneth L. Kiper.

8. "Loviisa Plant backfitting due to Shutdown PSA"; Internal Note, Loviisa NPP.

9. "Compendium of Practices on Safety Improvements"; B. Tomic, Presentation to the OECD-NEA PWG 5, September 1996.

10. "Shutdown and Low-Power Operations for Nuclear Power Reactors"; NRC 10 CFR Part 50, Federal Register Vol. 59 No. 201, October 1994.

11. "Shutdown and Low-Power Safety Assessment - A Status Report"; U. Hauptmanns, GRS, August 1993.

12. "Nuclear Power Reactors in the World"; IAEA, April 1995.

13. "Approaches and Results for Recent Shutdown Risk Studies in the U.S."; Nelson A. Hanan and Alan S. Kuritzky.

14. "SEPRA - Shutdown PSA for Olkiluoto NPP"; Risto Himanen, 1995.

15. "Shutdown Probabilistic Safety Assessment for Sizewell 'B' Nuclear Power Plant"; M.L. Ang, A.K. Brook and D.B. Utton, 1995.

16. "Safety Improvements and Operation Optimization Based on Shutdown PSA"; Lars Bennemo, 1995.

17. "PSA for the Shutdown Mode for Nuclear Power Plants"; IAEA TECDOC-751, June 1994.

18. "Analysis of Accident Sequences in Shutdown States for the Doel 3 and Tihange 2 PSAs"; P. Fossion and P. de Gelder, December 1992.

19. "Guidelines for Shutdown Risk Assessment"; IAEA working material, 1994.

20. "Procedures for Probabilistic Safety Assessment for Shutdown and other Low-Power Operating Modes"; IAEA working material, 1995.

21. "EPZ Integrated PSA Report No.: PSA3-94-1"; Borssele NPP, 1994.

22. "The Sizewell B Shutdown Probabilistic Analysis"; A.K. Brook, presentation to the IAEA Technical Committee Meeting, November 1994.

23. "Level 1 PSA for Japanese Typical 1,100 MWe PWR Plant During Low-Power and Shutdown Operation"; Tetsuji Kumano and Mitsumasa Hirano, (Institute of Nuclear Safety and Nuclear Power Engineering Corporation), Japan, 1995.

24. "Identification of Adverse Initiating Events in PWR During Low-Power and Shutdown States and the Assessment of their Consequences on Plant Safety"; Manfred Simon, 1995.

25. "Results of the Goesgen Level 1 PSA for Nonfull-Power Conditions"; Shobha b. Rao and Jurg Landolt, 1995.

26. "Methods and Lessons Learned from Doel 3 and Tihange 2 SPSA's"; H. Delsoir Fossion, 1995.

27. "Needs of Update of NEA SPSA Report"; ENCONET Consulting 1995.

7.2 Other Sources

Information from the following sources has also been used in the preparation of this report:

1. On UK (Sizewell B NPP) experience and findings: private communications between ENCONET Consulting and Mr. K. Brook and Dr. P.J. Ross.

2. On USA (Seabrook NPP) experience and findings: private communications between ENCONET Consulting and Mr. K. Kiper.

3. On USA experience and findings: Private communications between ENCONET Consulting and Mr. Bengt Lydell.

4. On German (KGB Gundremmingen NPP,) experience and findings: private communications between ENCONET Consulting and Mr. Geßler and Mr. R.M. Zander.

5. On Belgium experience and findings: private communications between ENCONET Consulting and Mr. Peter de Gelder.

6. On Belgium (Doel NPP) experience and findings: private communications between ENCONET Consulting and Mr. L. Rogghe.

7. On Belgium (Tihange 1-3 NPP) experience and findings: private communications between ENCONET Consulting and Mr. A. Lousberg and Mr. L. Vandermeeren.

8. On Spanish (Vandellos II NPP) experience and findings: private communications between ENCONET Consulting and Mr. M. Otero.

9. On Spanish (Asco 1-2 NPP) experience and findings: private communications between ENCONET Consulting and Mr. Jose Faig.

10. On Finnish (Loviisa NPP) experience and practice: private communications between ENCONET Consulting and Mr. J.K. Vaurio.

11. On Finnish (TVO I/II NPP) experience and findings: private communications between ENCONET Consulting and Mr. Risto Himanen.

APPENDIX A - COMPARISON OF IMPROVEMENTS BY CATEGORIES

SAFETY AREA	ADMINISTRATIVE IMPROVEMENTS	HARDWARE IMPROVEMENTS	OPERATIONAL IMPROVEMENTS
MINIMISING THE PROBABILITY OF AN IE			
LOCA	- The pressuriser manway to be the first large opening on RCS, to prevent a rapid core uncovery by a piston effect	- New equipment for removal of control rod drives through lower personnel access door. - Cotter Pin plugs are installed for the Main Circulation pumps to prevent an inadvertent lifting with a miscalibrated crane - Modifications of the maintenance equipment for the Main Recirc Pump	- Reduce the probability of LOCA by op. Procedure related to draining of the cavity - The practice for inspection control rods was modified to reduce the possibility of inadvertent loss of coolant - The test procedure for isolation valves was enhanced - Limit the manipulation of systems connected to RCS
Loss of RHR	- Technical Specifications revised to ensure that there is no initial degradation of the RHR (all equipment shall available) when SG Cooling is no longer used.	- Install mobile ultrasonic level sensor on hot leg - Install interlock to automatically terminate draining of reactor cavity, upon low level signal - Improve water level measuring equipment for mid loop - A diverse and more accurate level measurement parameter engineered to control the mid-loop level - Increase the margin-to-vortex for RHR pumps by raising water level and reducing the set point for RHR - Installation of an early warning of vortex at RHR pumps - Implementation of an ultrasonic water level measurement system for mid-loop operation - Improved the reliability of the mid-loop water level measurement system - Inhibition of the protection signal for cavitation of RHR pumps for the mid-loop operation - Improvement in the water level measuring equipment (permanent installation) for mid loop operation	- Op. procedure for verification of przr. level control (redundant level measurement during shutdown). - Procedural requirement for a specific sequence when installing SG nozzle dams, including required clearance with the control room. - Limited manipulation of systems which support the operation of RHR. - Reduce the probability of drainage of reactor by increased training of operators on manipulations relative to changing the water level.
Loss of power	- Technical Specifications require the availability of two off-site and two on-site electrical power supplies;		
Reactivity incident	- Required level of redundancy for neutron flux source range monitoring system. - Complete isolation of CVCS is required after all RCP switched off.	- Improvement of the boron treatment system to prevent boron dilution events. - Improvement of instrumentation for measuring the boron acid concentration in the RCS. - The suction of CVCS was switched to RWST	- Procedure for isolation of CVCS after all the RCPs have been switched off - Procedures to prevent injection of non-borated coolant during start-up - Guidance for shift personnel to assure that no inadvertent dilution has occurred before starting a RCP.

SAFETY AREA	ADMINISTRATIVE IMPROVEMENTS	HARDWARE IMPROVEMENTS	OPERATIONAL IMPROVEMENTS
MINIMISING THE PROBABILITY OF AN IE			
Over-pressurisation	- Use of the auxiliary feedwater pumps for filling the reactor above certain level is forbidden - Lock closing of the safety/relief valves before removal of the reactor lid is forbidden	- A diverse pressure relief paths has been engineered	- Procedure to use low pressure pumps to fill the RV - Procedure to ensure that the pressuriser heater banks and HPSI are switched-off during Cold Shutdown - Change the timing of tests for pressuriser relief valves - Procedure related to SG tightness test, to allow the operator to concentrate on specific function
Others	- All the procedures and technical specifications related with the shutdown operations were reviewed for their relevance considering the results of SLP PSA.		- Modification of procedures related to tests which are allowed in shutdown conditions - Training of the outage personnel to understand the risks related with shutdown operations - Modification of practices of heavy load lifting - Outage is defined a project with information on different activities and safety during outage - A specific set of operating procedures for the shutdown states was developed.
INCREASED AVAILABILITY OF MITIGATING SYSTEMS			
Heat removal	- At least one SG is required to be operable to remove residual heat until a prszr manway is removed - Spent Fuel Pit Cooling must be available to back up the RHR system while prsrz manway is open. - Maintain the water level in at least one SG before full opening of the RCS - Availability of bunker during critical phases of outage - At least one SG shall be available during POS 4, 5, 6 Introduction of administrative controls to assure the availability of the alternative cooling methods	- Improved reliability of the RHR system - Use of the well water cooling with the RHR system, to have independent ultimate heat sink during shutdown	- Incident EOP for recovery of vortex on RHR (before the automatic initiation of the water supply) - Accident EOP for recovery of the total loss of RHR - Operating procedures to cover for alternative cooling - Operating Procedures for Loss of RHR. - Operating Procedure for Loss of RHR at Mid-loop - Operating Procedure for loss of RHR heat exchanger - Procedure for refill after a complete loss of the RHR. Use of all three redundancies of RHR (including RHR train of SFP) when the core is in the vessel
Inventory control	- Increased availability RCS water supply: 2 CVCS and 2 LPSI injection lines are required to be available - 3 out of 4 core spray trains are required to be available during critical steps of the outage - Technical Specifications require periodic verification of sources of water throughout the outage - Requirements for the availability of accumulators Available ECCS and its alignment for hot leg injection is required to enter the mid-loop operation.	Automatic initiation of the RCS water supply, upon the loss of RHR pumps (low-low level RHR flow rate and low pressure at the RHR pumps discharge)	- Procedure for using the gravity feed from the RWST - Operating instructions for operators to mitigate the consequences of small LOCA before RCS level drops under the mid loop level - Operating instructions for small LOCAs in shutdown - EOP enhanced to address LOCA and loss of RHR events during shutdown - Improvement of Operating Procedure for LOCA in Modes 3 and 4

SAFETY AREA	ADMINISTRATIVE IMPROVEMENTS	HARDWARE IMPROVEMENTS	OPERATIONAL IMPROVEMENTS
INCREASED AVAILABILITY OF MITIGATING SYSTEMS			
Other	- TS in the same format as for power cover all the activities with coolant temperature below 100 C. - Umbrella schedules for maintenance activities on systems/trains are prepared for every outage - TS developed for all shutdown modes. 55 TS items relevant for modes 4, 5, 6. - Equipment availability requirements in TS. In shutdown availability requirements less that for full power. (4/4 HPSI at power; 1 for LPS, another operable but discharge valve closed and electric supply isolated - Schematics for core cooling, core flooding and electrical supply for outage. These are used in the CR	- Bunker systems designed to start automatically for external events consideration during shutdown - Test lines installed for the check valves of the ECCS and CS System - Condition monitoring systems used for determining condition of equipment before maintenance	- Specific work procedures introduced for shutdown. - Specific training on em. procedures for shutdown - Umbrella system with specific shutdown and start-up procedures for components and systems - Testing schemes developed to assure the operability of equipment after maintenance - Test procedures established for check valves of ECCS and CS System - Op. plan prepared for every outage indicating required operability of systems during shutdown operation
ENHANCED RECOVERY CAPABILITY			
Increased time available for recoveries and early warning	- Additional TS limiting duration of mid loop operations. - Time limitation on RCS openings to ensure the decay heat level is below 1 hr to core uncovery - Improvements of the administrative controls to minimise the time in the low water configuration - Modification of activities during mid loop, reduced critical configurations during mid loop operation	- Specific alarm was installed for cavitation of running RHR pump	- Specific instructions related to operators' mitigation of the boron dilution sequences within prescribed time (before the criticality) - Two specially trained guards are posted at the access door of the lower equipment personnel access for the full duration of the pump overhaul (to limit the consequence of LOCA) - See also the entries under "Increased availability..""
Enhanced status control	- Continuous monitoring of selected parameters: RCS level, core exit and RHR system temperatures, RHR system operation - TS modified to require periodic verification of water level throughout the outage.	- Installation of a permanent monitoring of the cavity and the RCS level from the control room - Enhancement of the water level instrumentation and other alarms to support operators and improve the response time to an (incipient or actual) loss of RHR during the mid-loop operation	- See also the entries under "Increased availability..""
Other	- Use of ORAM tool to reduce the configuration related risks during outages		- Specific procedures were introduced for mid-loop operation. - "Operational Commitments " data base produced collecting all the requirements for shutdown

SAFETY AREA	ADMINISTRATIVE IMPROVEMENTS	HARDWARE IMPROVEMENTS	OPERATIONAL IMPROVEMENTS
IMPROVED CONTAINMENT			
Containment closure capabilities	- The confinement function must be maintained while the fuel in the core (the containment hatch may be open, but must be possible to re-close if necessary - TS to ensure containment integrity while at mid-loop - Administrative controls on containment integrity - Requirement to keep the containment equipment hatch closed during the mid lop operation from the removal of the SG manway to installation of the last nozzle dam		

APPENDIX B LIST OF ENHANCEMENTS FOR SHUTDOWN OPERATION OF NPPS

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
French PSA Studies (1990) 900 MWe and 1300 MWe	1. Highlighted the importance of shutdown and low power operation. 2. Identified high contribution to CDP from Loss of RHR 3. Identified high importance of Mid-loop operation, and loss of RHR in that mode 4. Identified the problems related with inaccurate vessel level monitoring 5. Confirmed that delaying critical operations greatly reduce the risk level 6. Identified specific mitigating actions **ACTION TAKEN:** French Safety Authority requested from the EdF to implement a set of measures which would reduce the risk of core damage to 10E-06/plant/year for shutdown operations.	**ADMINISTRATIVE** - Implementation of additional Tech. Spec. Requirements related to limiting the duration of mid loop operations. The aim is to minimise the probability of loss of RHR when water level below the vessel flange level. - Increased availability RCS water supply. - Diversity for DHR in RCS-closed condition: At least one SG is required to be operable (secondary side FW available) to remove residual heat (by re-flux condenser cooling mode with the presence of non condensable gas), until a prszr manway is removed. - Increased redundancy of RHR in RCS open condition: Spent Fuel Pit Cooling and Treatment System (SFPCTS) must be available to back up the RHR system while prsrz manway is open. - Minimise the probability of loss of power event: Technical Specifications were modified to require the availability of two off-site and two on-site electrical power supplies; - Introduction of a requirement that the first large opening of RCS is in a hot leg. This is meant to prevent a rapid core uncovery by a piston effect (when there is a opening on the cold side, while there is no opening on the hot side). - Introduction of time limitation on RCS openings to ensure that the decay heat is reduced to a level that there is a minimum of one hour of delay to core uncovery in case of loss of RHR. - Minimise the off-site consequences: The confinement function must be maintained while the fuel in the core (the containment hatch may be open, but must be possible to re-close if necessary before a core damage is to occur). **HARDWARE** - Installation of a permanent monitoring of the cavity and the RCS level from the control room. For each cold shutdown, when the RCS is to be opened, the utility has installed a precise and reliable level measurement, with an ultrasonic probe which has a contact with the primary hot leg. (This is meant to replaces mobile ultrasonic level measurement). This measurement shall provide a low level alarm in the control room. - Installation of an early warning of vortex at RHR pumps. Measurement of the pressure fluctuation at the discharge of RHR pumps is considered representative of an impeding vortex on pumps. (This provides a diversity for the reactor level measurement). The alarm from this system initiates the application of an appropriate incident emergency operating procedure, and evacuation of the containment. - Installation of an interlock which shall automatically terminate the draining of the reactor cavity draining, on the cavity low level signal. - Increase the margin -to-vortex for RHR pumps: Raise the water level for mid-loop operation and reduce the set point for the RHR low flow. - Automatic initiation of the RCS water supply, upon the loss of RHR pumps (low-low level RHR flow rate and low pressure at the RHR pumps discharge, both to be alarmed in the control room), with the RCS level is below the reactor flange. At 1300 MWe series, a Low Pressure Safety Injection (LPSI) pump is used for this purpose.

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
French PSA Studies (1990) 900 MWe and 1300 MWe	**So-called "93 set of modifications" (hardware improvements) to be implemented between 1994 and 1998.** **All of these measures will be implemented between 1994 and 1998 and completed by:** **French Safety Authority position:** 1. Considers that it is possible to relax some operating constrains as proposed by utility. **Utility (EdF) is carrying out some studies aiming to resolve these issues:**	**OPERATIONAL** - Reduction of the probability of loss of coolant by enhancement of the operating procedures governing the activities related to draining of the reactor cavity. - Enhancement of the (incident) EOP for recovery of vortex on RHR pumps (this procedure is relevant before the automatic initiation of the water supply). - Enhancement of the (accident) EOP for recovery of the total loss of RHR (after the failure of "incident" EOP. - Limitation in allowed manipulation of systems connected to the RCS or systems which support the operation of RHR. - Reduction of the probability of accidental drainage of reactor by increased training of operators on manipulations relative to changing the water level in the reactor and the cavity. **ENHANCEMENTS UNDER CONSIDERATION** - Relaxation of the delay required before opening the vents (partially open configuration) from 2 days to 1 day after Shutdown. (A comprehensive TH study with CATHARE code is required to justify the request). - Relaxation of the requirements for the core exit temperature measurement. - Relaxation of the containment opening requirements: the containment may be open when the RCS is partially open and must be re-closable (before core uncovery) when the RCS is open. **ADDITIONAL ANALYSIS** - Additional analysis to determine if the boron crystallisation phenomena contribute to risk of failure of a transition to simultaneous injection using SI system. - Additional analysis to determine the effectiveness of the automatic water supply, considering the spectrum of initiators which could lead to the loss of RHR (and may impact the ability to supply the water form other sources) - Complete probabilistic reassessment to determine the specific contributions to risk during RHR cooling mode from all initiators as well as the relative contribution of the long term mission times - Additional analysis to optimise the containment opening management considering the overall risk profile.

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Surry-1 **USA**	1. The maintenance activities during the Mid-loop conditions was identified as the dominant risk contributor. The POS is characterised by a high decay heat level and relatively short time available for operator action. 2. The gravity feed from the RWST could be used to remove the decay heat. The gravity feed is enough for a long term cooling (24 hr) only when the decay heat is relatively low. However, it can provide a margin of a few hours for restoring other means of decay heat early in an outage. 3. Check lists reduces the impact of maintenance unavailability. 4. The water level instrumentation used during Mid-loop operation, i.e. standpipe level instrumentation and ultrasonic level instrumentation, have limited applicability during an accident. 5. Isolation of the RCS loops contributes to core damage frequency during the Mid-loop operation., due to reduced availability of SGs.	**ADMINISTRATIVE** - The utility focused on review of the outage practices which required extensive activities during mid loop operation, and reduced critical configurations during mid loop operation. The outage schedule was modified to drastically reduce the duration of the Mid-loop configuration. **OPERATIONAL** - Various administrative requirements and work procedures were introduced or existing procedures modified. - A procedure for using the gravity feed from the RWST enhanced.
Seabrook **USA**	1. Loss of RHR is the largest contributor to CDF (82%) 2. The highest contributor to loss of RHR is hardware failure in running RHR train. (This is a consequence of a relatively long mission rather than a high failure rate of the RHR). Loss of the RHR suction is only the second highest contributor. 3. Loss of RHR events with the RCS vented/partially drained contribute to CDF with 71% 4. RCS vented/partially drained configuration is the most important one at Seabrook. 5. LOCA contribute to CDF with about 18%. About 8% comes from the over-pressure events. 6. The cold-pressurisation is not a reactor vessel or piping integrity concern; It has a high potential for the RHR relief valve to stuck open or the RHR pump seal to rupture. 7. LOCAs are important contributors to early health risks. This is due to the containment equipment hatch being allowed to be open during re-pressurisation. 8. The results show that the risk is very sensitive to the reliability of the operators.	**ADMINISTRATIVE** - Administrative controls to minimise the time in the low water configuration, - Introduction of administrative controls to assure the availability of the alternative cooling methods - Introduction of the administrative controls on the containment integrity. **HARDWARE** - Enhancement of the water level instrumentation and other alarms to support operators and improve the response time to an (incipient or actual) loss of RHR during the mid-loop operation. **OPERATIONAL** - Improvements of the operating procedures to cover for the abnormal plant conditions and alternative cooling schemes. - Introduction of specific training on emergency procedures for shutdown operations

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
TVO 1-2 **Finland**	1. Leakage below the core is dominant contributor to the CDF ; (68%). 2. Leakage above the core is a visible contributor to CDF (9.%.) 3. Loss of RHR System is high contributor; 22.51%. 4. Fuel damage in SPF is insignificant. 5. The beginning of a refuelling outage is an important contributor to risk 6. A risk peak occurs during the-filling of the reactor (with reactor lid closed) and during the first days of maintenance activities. 7. The Human interaction is a dominant contributor to risk with over 90% contribution. The importance of human actions was confirmed through the sensitivity analysis.	**ADMINISTRATIVE** - To increase the capability of waster supply in case of a LOCA, 3 out of 4 core spray trains are required to be available during critical steps of the maintenance of the main circulation pumps. Generally, availability of 1 out of 4 trains of the core spray is required during an outrage. - The Technical Specifications were modified to require periodic verification of the water level and the available sources of water throughout the outage - The use of the auxiliary feedwater pumps for filling the reactor above certain level is forbidden. This greatly reduce the possibility of cold over-pressurisation. - Lock closing of the safety/relief valves before removal of rather reactor lid is forbidden. This greatly reduce the chance of overpressurisation. **HARDWARE** - New equipment for removal of control rod drives through the lower personnel access door is used. This allow for easier and faster door closure. - Cotter Pin plugs are installed for the Main Circulation pumps to prevent an inadvertent lifting, with a miscalibrated crane (which may cause a massive leakage). - Numerous small modifications were introduced on the maintenance equipment for the Main Recirculation Pump. **OPERATIONAL** - The practice for inspection control rods was modified to reduce the possibility of inadvertent loss of coolant - Emergency operating procedures were enhanced to address LOCA and loss of RHR events during shutdown. - Two specially trained guards are posted at the access door of the lower equipment personnel access for the full duration of the pump overhaul. This allows for the only recovery action (closure of the door) in case of massive primary leak. - The test procedure for the isolation valves was enhanced. - Training of the outage personnel to understand the risks related with shutdown operations).

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Loviisa **Finland**	**NOTE:** The Loviisa SLP PSA is not completed yet. No actions have been taken based on quantitative analysis. However, during the course of the identification of hazards, several items were identified which are risk important. Immediate changes of procedures was initiated (control room Start-up procedure, primary loop level control procedure, several test procedures, etc.). While performing the Full-Power PSA, some obvious initiators during Shutdown have been considered. As a result, some plant modifications were implemented.	**ADMINISTRATIVE** - Improvement (modification) of the Technical Specifications especially related with issues where operational practices was causing the violation of safety requirements. - Administrative requirements on level of redundancy for neutron flux source range monitoring system. - Administrative requirements for the availability of accumulators. **HARDWARE** - Improvement of the boron treatment system to prevent boron dilution events. **OPERATIONAL** - Modification of the procedure for calibration and verification of the pressuriser level control (redundant level measurement during shutdown will be implemented). - Modification of the procedure for monitoring of core outlet temperature during critical phases of an outage (e.g. reactor vessel head open). - Modification of the procedure to ensure that the pressuriser heater banks and HPSI are switched-off during Cold Shutdown (prevention of overpressurisation). - Modification of the procedures related to the requirements for tests which are allowed in ambivalent conditions (prevention of Cold over-pressure mainly). - Procedural requirements to keep SG available to enable cooling via SGs. - Change the timing of tests for pressuriser relief valves to reduce the probability of cold overpressurisation. - Improvement of procedures and administrative controls to prevent injection of non-borated coolant during start-up. - All heavy load lifting and transport operations during shutdown have been reviewed and assessed for their risk contribution. This led to modifications in operating routines and practices.
Vandellos II **Spain**	1. Implemented improvements based on recommendations of "Westinghouse Owners Group" and on operating experience. 2. Implemented improvements based on plant specific SLP PSA.	**ADMINISTRATIVE** - Maintain the water level in at least one SG before full opening of the RCS. **HARDWARE** - Implementation of an ultrasonic water level measurement system for mid-loop operation. **OPERATIONAL** - Improvement of Operating Procedures for Loss of RHR (POF-112). - Improvement of Operating Procedure for Loss of RHR at Mid-loop operation (POF-117). - Improvement of Operating Procedure for LOCA in Mode 3 and 4 (POF-118). - Extend the applicability of Operating Procedure POF-118 to operation in Mode 5 with pressure control with the pressuriser. - Improvement of Operating Procedure POF-112 (to include an additional malfunctions), related with the loss of RHR heat exchanger capability.

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Ringhals 4 **Sweden**	NOTE: A limited analysis addressing only selected activities (MCP Overhaul, Cold Over-pressurisation, refuelling, Control Rod Drive Overhaul, testing and inspections). and plant operational stages was performed using Barrier Analysis approach	**ADMINISTRATIVE** - Requirement to keep the containment equipment hatch closed during the mid lop operation from the removal of the SG manway to the installation of the last nozzle dam. **OPERATIONAL** - Modification of the RCS filling procedure to use only the low pressure pumps to prevent the overpressurisation. - Improvement of the procedure related to SG tightness test, to also the operator to concentrate on the specific function. - Procedural requirement for the specific sequence in which the SG nozzle dams must be mounted, including a requirement for a clearance with the control room. This is to prevent forming of a steam bubble and uncovery of the core in case of a loss of RHR.
Ringhals 2 **Sweden**	1. High value for "Severe safety consequence" in shutdown with the dominant sequence being Loss of RHR during Mid-loop operation. 2. Failure of operators to recover specific sequences is a high contributor. 3. Detailed sequence analysis additionally considered alternative Heat Removal Paths,. Re-quantification reduced CDF for about an order of magnitude.	**HARDWARE** - Improvement in the waster level measuring equipment (permanent installation). For mid loop operation (this improvement was decided before the Shutdown study) **OPERATIONAL** - Specific procedures, and instructions were introduced with regard to the Mid-loop operation. - Operating instructions for operators to mitigate the consequences of small LOCA before RCS level drops under the mid loop level - Operating instructions for small LOCAs in hot and cold shutdown - Introduction of specific instructions related to operators' mitigation of the boron dilution sequences within prescribed time (before the criticality)
Barseback **Sweden**	1. SPSA study performed using PSA approaches. (Results and insights not available) 2. The safety improvement initiated before the study and modified to account for the results of the analysis	**ADMINISTRATIVE** - Technical specifications having the same format as for the power operation was developed to cover all the activities with coolant temperature below 100 C. - Operational plan for shutdown period is prepared for every outage indicating required operability of systems during shutdown operation - Schematics for core cooling, core flooding and electrical supply are developed for specific outage periods. These schematics are used in the CR for controlling the operation of specific systems - Umbrella schedules for maintenance activities on complete system or a series or interconnected systems/trains are prepared for every outage **HARDWARE** - Additional spare parts are used on specific component during outages - Condition monitoring systems are used for determining exact condition of equipment before embarking on maintenance operations **OPERATIONAL** - Umbrella systems with specific shutdown and start-up procedures for components and systems was prepared and is used regularly - Post maintenance testing schemes were developed and used to assure the operability of equipment following the maintenance activities - Every outage is defined a project with its own management and project handbook with information on different activities and safety during outage

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Doel 3 **Thiange 2** **Belgium**	1. The core melt frequency during the Shutdown states is not negligible contributor to overall risk 2. Human interaction contributes significantly to the core damage frequency in shutdown 3. When considering diagnostic errors, specially at Mid-loop operation, this contribution is even higher 4. Mid-loop operational state is a very high contributor. 5. Inadvertent drainage and Loss of RHR System are the dominant accident sequences. 6. The benefit of the Bunker systems is significant (ECCS DGs) despite of potential negative effect at Mid-loop operation. **Risk distribution between Shutdown Initiating events:** Drainage; 46%. Loss of RHR System; 26%. LOCA's; 19%. Station Black Out; 5%. Loss of CCW System; 4%.	**ADMINISTRATIVE** - The availability of ECCS and its alignment for a hot leg injection is required to enter the mid-loop operating state. **HARDWARE** - Inhibition of the protection signal for cavitation of RHR pumps for the mid-loop operation - Bunkerised safety systems were designed to start automatically fro external events consideration during shutdown - Specific alarm was installed for cavitation of running RHR pump - Test lines were installed for the check valves of the ECCS and CS System **OPERATIONAL** - A specific set of operating procedures for the shutdown states was developed. - Test procedures was established for the check valves of the ECCS and CS System
Borssele **The Netherlands**	1. Mid-loop operation is the POS with the highest contribution to outage risk. 2. The differences between the long-cycle- and the short-cycle-outages are small and are mainly the results of the differences in the duration of the power cycles. 3. The Core Damage Frequency during shutdown operation is dominated by fire initiators.	**ADMINISTRATIVE** - All the procedures and technical specifications related with the shutdown operations were reviewed for their relevance considering the results of SLP PSA. - Modification of the operability requirements was introduced to assure availability of bunker system during critical phases of outage. **HARDWARE** - Improved the reliability of the Midloop Water level measurement system - Improved reliability of the Residual heat removal system, - Additional connection to enable use of the well water cooling with the residual heat removal system, to have independence for the ultimate heat sink during shutdown operation

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Sizewell B **United Kingdom**	1. Contributions to CDF during shutdown at Sizewell are: - Loss of Decay Heat Removal; 36%. - Internal Fire; 27%. - Boron Dilution Faults; 12%. - Seismic Events; 10%. - LOCAs; 4%. - Cold Over-Pressurisation Faults; 1%.	**ADMINISTRATIVE** - Sizewell B uses ORAM tool to reduce the configuration relate risks during outages - Technical specifications were developed for all shutdown modes. 55 out of total of 100 tech Spec items rare relevant for modes 4, 5, 6. Systems covered include Boron dilution, Cold over-pressurisation, Mid loop level measurement, RCP seal protections, SIS, EDG, CCW, protection and control etc.) - Equipment availability requirements for all modes were derived and new Tech. Spec produced. In shutdown some availability requirements were less that for full power. (For example, 4 to of 4 HPSI trains are required of power; 1 train required for LPS, with another operable but discharge valve closed and electric supply isolated) **HARDWARE** - To protect against boron dilution , the suction of CVCS was switched to RWST - To protect against cold over pressurisation, a diverse relief paths has been engineered. - A diverse and more accurate level measurement parameter has been engineered to help control the level when going mid-loop **OPERATIONAL** - Assumptions made in PSA and safety case were listed and inserted in operational documents - “Operational Commitments “ data base was produced collecting all the requirements which were not warrant production of a technical Specification requirement.
German reference plant **Germany**	1. With loss of RHR during mid loop operation, available time for countermeasures to prevent core uncovery is only 35 minutes. 2. Boron dilution events of relevance are those when a slug of unborated water is transported to the core. Such event may cause fuel damage and/or high pressure peaks, 3. Fast boron dilution accounted are of very low frequency 4. Loss of RHR can easily be detected by physical observations (e.g. by RHR Pump failure, coolant temperature increase). 5. Unintentional dilution of the RCS may be difficult to detect before a increase of neutron flux (criticality). 6. Mitigation measures may be initiated too late or may have no effect with regard to the safety situations of the plant.	**ADMINISTRATIVE** - At least one SG shall be kept available during POS 4, 5 and 6 - For the prevention of boron dilution events, complete isolation of CVCV is required after t all RCP having been switched off. **HARDWARE** - Improvement of the instrumentation for measuring the boron acid concentration in the RCS. **OPERATIONAL** - Accumulators shall be used for refill after a complete loss of the RHR. - Additional guidance for shift personnel to assure that no inadvertent dilution has occurred before starting a RCP.

Nuclear Power Plant	Results/Findings of SLP PSA	Enhancement/improvements proposed or implemented
Goesgen **Switzerland**	**NOTE:** The results are expressed in terms of events per calendar year to measure the annual average fuel damage frequency, and, as such, include an estimate of the fraction of time in a year that the plant is in different configurations. Fuel Damage Frequencies (CDF) (mean values, per year) are as follows: 1. RHR Phase with Core in Vessel; 3.390E-05. 2. RHR Phase with Core in Pool; 4.890E-05. 3. RHR Phase with Core Flooded Cavity; 9.710E-06. 4. Cool-down on Heat-up Phase P<40%; 1.560E-08. **Results/Findings:** 1. The annual average frequency of CD in shutdown modes other that the Cool-down and Heat-up Phases is be significantly greater than for the full power operation. 2. Internal initiators (random hardware failures) that cause a Loss of the RHR are the most important group (55%) followed by internal fires (31%) and internal events with LOCA (11%). Other external events are much less important (3%). 3. Loss of RHR due to internal initiators was found to be most important for conditions with the core in the vessel and in the spent fuel pool. 4. Internal fires and internal events causing a drain-down condition were dominant for the refuelling cavity flooded configuration. 5. Almost all of the contribution to damage during the type B outage (forced outages greater than 24 hours with opening of the RCS) comes from Mid-loop operation. 6. Forced outage type B was found to have the highest conditional CDF because of the possibility permitted by current Technical Specifications of entering such an outage with only one RHR cooling train available to cool reactor vessel (second RHR is available, but it is aligned to cool Spent Fuel Pool).	**ADMINISTRATIVE** - Technical Specifications to be revised to ensure that there is no initial degradation of the RHR (all equipment available) when SG Cooling is no longer used. **OPERATIONAL** - Better use of all three redundancies of the RHR System (including the RHR train cooling the Spent Fuel Pool) when the core is in the vessel and the decay heat level of the fuel in the Pool is low.